Towards the Internet of Things Forensics: A Data Analytics Perspective

Pimal Khanpara[1], Ishwa Shah[1], Sudeep Tanwar[2], Amit Verma [3], and Ravi Sharma[4]

[1]Nirma University Institute of Technology
[2]Nirma University of Science and Technology Institute of Technology
[3]Chandigarh University
[4]UPES

January 30, 2024

Abstract

The widespread use of networked, intelligent, and adaptable devices in various domains, such as smart cities and home automation, climate control, manufacturing and logistics, healthcare, education, and agriculture, has been hastened by recent developments in hardware and software technologies. In all these application domains, the concept of the Internet of Things (helps to achieve process automation and decrease labor costs. One such subdomain is IoT Forensics which involves Digital Forensics concerning IoT devices, networks, or clouds. In this process of obtaining substantial evidence from the devices, networks, or cloud, a large amount of data and operations on said data are involved. Hence, looking through IoT Forensics through the methodology dealing with data, known as Data Analytics, is essential. This paper presents an interpretation of IoT Forensics from the standpoint of Data Analytics. To explain the same in detail, the paper focuses on IoT Forensics, its methodologies, and how they relate to data analytics stages. Towards the end, the paper discusses current developments in IoT forensics from the Data Analytics perspective, limitations observed in the existing technologies, adoption challenges, and possible future advancements.

Received ; | Revised ; | Accepted

DOI: xxx/xxxx

RESEARCH ARTICLE

Towards the Internet of Things Forensics: A Data Analytics Perspective

Pimal Khanpara[1] | Ishwa Shah[1] | Sudeep Tanwar*[1] | Amit Verma[2] | Ravi Sharma[3]

[1]Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, 382481, Gujarat, India (pimal.khanpara@gmail.com, 18bce218@nirmauni.ac.in, sudeep.tanwar@nirmauni.ac.in)

[2]Department of Computer Science Engineering, University Centre for Research & Development, Chandigarh University, Mohali, Punjab, India. (amitverma.121287@gmail.com)

[3]Centre for Inter-Disciplinary Research and Innovation, University of Petroleum and Energy Studies, Dehradun, 248001, India (ravisharmacidri@gmail.com)

Correspondence
*Sudeep Tanwar, Email: sudeep.tanwar@nirmauni.ac.in

Abstract

The widespread use of networked, intelligent, and adaptable devices in various domains, such as smart cities and home automation, climate control, manufacturing and logistics, healthcare, education, and agriculture, has been hastened by recent developments in hardware and software technologies. In all these application domains, the concept of the Internet of Things (helps to achieve process automation and decrease labor costs. While Io T has been an established domain for quite a while, it has seen a lot of advances and challenges in different subdomains over the years. One such subdomain is IoT Forensics which involves Digital Forensics concerning IoT devices, networks, or clouds. In this process of obtaining substantial evidence from the devices, networks, or cloud, a large amount of data and operations on said data are involved. Hence, looking through IoT Forensics through the methodology dealing with data, known as Data Analytics, is essential. This paper presents an interpretation of IoT Forensics from the standpoint of Data Analytics. To explain the same in detail, the paper focuses on IoT Forensics, its methodologies, and how they relate to data analytics stages. Towards the end, the paper discusses current developments in IoT forensics from the Data Analytics perspective, limitations observed in the existing technologies, adoption challenges, and possible future advancements.

KEYWORDS:
Internet of Things (IoT), IoT Security, Digital Forensics, IoT Forensics, Data Analytics.

1 | INTRODUCTION

Technological advancements have reached a new high in the past decade. And, with these advancements, so has the dependency they have created on our lives. Not only that, new dependencies and needs have been created with their increased usage. One such advancement in technology observed over the past decade is the Internet of Things (IoT)[1 2]. The concept of IoT describes a dynamic ecosystem of connected computing devices with various components enabling smooth communication and data exchange. In general, IoT refers to physical objects with sensors, computing power, software, and other technologies that can link to other systems and devices via the Internet or other communication networks and exchange data with them. Physical objects used in the deployment of IoT often include smart wearable devices for health monitoring, Radio Frequency Identification Technology (RFID) tags, sensors to measure various parameters based on application-specific requirements, and other components through which proactive sensing and processing can be accomplished. Today, IoT is an integral part of the

Computer Science domain and a component of daily life. Internet of Things is, according to the European Researchers Cluster on the Internet of Things (IERC), a self-configuring, wise-to-change, global network infrastructure by the standard and backward compatible communication protocols, in which both physical as well as virtual things have identities, physical attributes, and virtual personalities and at the same time, use intelligent interfaces, and are impeccably consolidated into the information network.

Contingent upon different advances in usage, the meaning of the "Internet of Things" shifts. In any case, the principle of the IoT suggests that objects in an Internet of Things can be distinguished extraordinarily in virtual portrayals. Inside the Internet of Things, everything is ready to trade information and, if necessary, measure information as indicated by predefined plans. Even though there are heterogeneous definitions of the understanding of the "Internet of Things", it has a comparing limit identified with the combination of the actual world with the virtual universe of the Internet. The Internet of things can extensively be characterized as a worldwide organization framework, connecting interestingly recognized physical and virtual items, things, and gadgets.

Even though it is already an established field, new technologies bring in demands for data connectivity, and new devices require new services that IoT has yet to offer. This brings forth further growth in the field in terms of both the hardware components and software elements. However, irrespective of the interdisciplinary domain that IoT has been incorporated into, most IoT applications and devices involve data collection in different forms. This data is susceptible to intruders and malicious intenders when transferred via a network. This introduces a possible trade-off between data collection using IoT, user security, and privacy[3]. Providing an efficient trade-off between the same imposes a new challenge, the demand for IoT Security[4 5]. In forensics, extracted logs or other data may be useful in cases involving IoT devices as key evidence in crime scenes and finding offenders. While IoT Security and IoT Forensics are important aspects of the Internet of Things domain, the paper focuses in-depth on IoT Forensics and how it can be perceived in terms of Data Analytics.

1.1 | IoT Security and IoT Forensics

Both IoT Security and IoT Forensics are domains of IoT that have great potential for the upcoming years. IoT Security ensures that IoT-based devices, networks, and cloud interfaces are secure[6]. IoT devices are connected through the cloud, and the internet, which makes them vulnerable to attacks in case of insufficient network as well as device-based protection against them[3 7 1]. IoT Forensics, on the other hand, deals with handling and reestablishing events through analysis of the different sources of events.

Whilst IoT Security involves quick real-time response to fend off potential and ongoing attacks by deploying various security techniques to ensure security against the threats in case of a live attack, IoT Forensics is generally of use after the incident. IoT Security is a generalized and continuous process, as there must be an all-time vigilance against threats. On the other hand, IoT Forensics essentially depends on the case. It comes into the picture only after the crime has occurred and until the case is solved.

On one hand, IoT Security is a relatively established domain under IoT, along with a constant need for security training and awareness in terms of security procedures and standards. IoT Forensics, on the other hand, is a relatively unexplored domain, with the requirement to meet the essential forensic needs to apply the standards while taking on an investigation such that the forensic value is maximized with minimal resource spending[8]. **FIGURE** 1 depicts the key differences between the IoT Security (IoT-S) and IoT Forensics (IoT-F) domains.

1.2 | The Concept of Digital Forensics

A subdomain of conventional forensics science is known as "Digital Forensics" (DF). It relates to the discovery and analysis of digital information. The significant tasks considered in Digital Forensics are identifying, gathering, recovering, analyzing, and preserving digital evidence from various electronic devices. All the aforementioned tasks must be executed in a specific sequence to follow the forensic investigation lifecycle. Various technologies and equipment are available to carry out the DF life cycle. Rapid data extraction and analysis accuracy are required to be ensured by the tools used in the investigation processes.

1.3 | Background of IoT Forensics

The branch of Digital Forensics that involves identifying, obtaining, and analyzing digital evidence, present in the form of a large amount of data, from the IoT devices for legal or investigative purposes is termed IoT Forensics[9]. While IoT Forensics is considered a sub-domain of Digital Forensics, it offers more evidence sources than standard digital forensics because of its

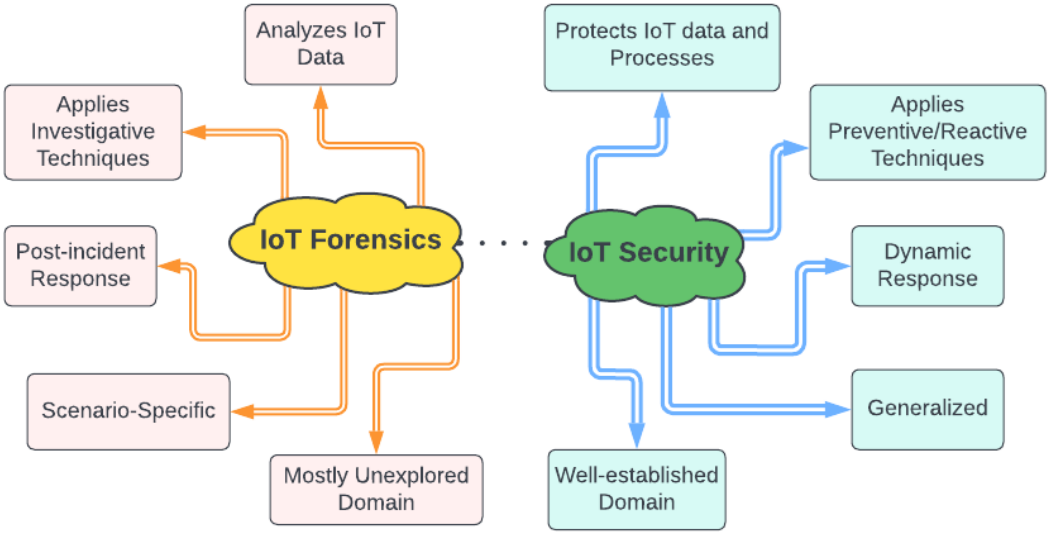

FIGURE 1 Key differences between IoT Forensics and IoT Security

interdisciplinary nature. Digital Forensics, under the broad umbrella, involves evidence found in digital format. IoT Forensics, on the other hand, is more linked to the environment through its different sources of evidence, as mentioned in this paper. The major differences between Digital Forensics and IoT forensics are listed in **TABLE**1 . The components of IoT-based devices,

TABLE 1 Basic Differences between Digital Forensics and IoT Forensics

Digital Forensics (DF)	**IoT Forensics (IoT-F)**
Long-established domain	Relatively young and less explored subdomain of DF
Conventional branch of forensics	Specialized branch of digital forensics
Deals with digital evidence	Focuses on devices to the Internet
Objects of investigation can be tablets, computers, smartphones, servers, or gateways	Evidence sources can include monitoring systems, device-to-device communication systems, sensors, Medical/Surgical body Implants, and any smart devices

such as sensors, that collect the data are the essential elements of the device [10]. This large amount of data collected from all such devices are sent directly to the Cloud. The storage is done through a connectivity medium, namely the various sources of Cloud-based connections such as Wi-Fi, Bluetooth, or satellite networks. The collected information is then analyzed on the Cloud and later sent to the end user to work on it. Throughout the entire process, a large amount of data is involved.

Although generally the availability of data through IoT devices, networks, or Cloud, it may even involve reconstruction of a chain of events or a given crime scenario, application of investigative techniques, or even usage in post-mortem investigation [11]. IoT Forensics is a time-restricted process that requires forensics readiness and falls under the judicial region that includes specification of legal aspects in legal service agreements regarding the forensic issues [8].

Based on the sources of evidence, the categorization of IoT Forensics includes:

- *IoT Device Level Forensics:* An investigator may need to gather data from IoT devices, particularly their local memory, at times. When it comes to collecting critical evidence from IoT devices, the device-level forensics scheme is used [12].
- *Network Forensics:* The source(s) of different assaults cannot be identified, in most cases, using network records. As a result, network logs are generally determined extremely useful in assessing whether a suspect is guilty. Various types of networks make up the IoT infrastructure, and it could be any of these that could provide critical pieces of information.

- *Cloud Forensics:* Cloud forensics makes up one of the primary aspects of IoT forensics. Since most IoT devices have limited processing and storage functionality, data captured through these IoT-based devices and networks are maintained and processed directly in the Cloud. This is mainly due to the significant benefits that cloud solutions provide, such as enhanced capacity, scalability, and on-demand accessibility.

Forensics, of any kind, needs to be handled carefully to ensure that there is no evidence of tampering of malicious intent or otherwise. Therefore, evidence needs to be preserved carefully. As we shall observe in detail in the later sections, the evidence of digital format and the sources of evidence included under IoT Forensics often face a trade-off between user privacy and investigation success.

1.4 | Motivations and Research Contributions

There is a massive potential for IoT security and forensics solutions. Several industries, such as intelligent transportation, home automation, microgrids, defense, healthcare, supply chain, and logistics management, operate on IoT-based solutions and, therefore, are susceptible to various attacks [13 14 15]. To deal with this, there is a need for efficient IoT security and IoT forensics mechanisms. As IoT forensics is a growing domain, there is a huge scope for research and development in this area. While searching for existing research regarding IoT Forensics, it was observed that very little research existed beyond the general challenges and approaches. Few researchers have worked in the domain of Data Analytics in IoT Forensics, even though IoT Forensics deals with such large amounts of data in the form of evidence.

Hence, motivated by the above facts, through this paper, the authors aim to contribute to research in the IoT Forensics domain by providing a comparison between individual stages of IoT Forensics and Data Analytics and, at the same time, briefing about the factors to be considered before incorporating the latter into the steps of the former. The major contributions of this paper are:

- A detailed taxonomy of IoT Forensics objectives, requirements, processes, and applications is presented.
- Existing research in IoT forensics, shortcomings, and possible means of improvement are explained in detail.
- The applicability of the Data analytics concepts in the IoT Forensics processes is discussed in depth.
- Real-life case studies depicting the need and importance of IoT Forensics through data analytics are covered in the paper.
- The challenges and key constraints in implementing the Data Analytics based forensic solutions are analyzed and presented to enable readers to carry out further investigations in the exploration of better outcomes.

1.5 | Organization of the Paper

The paper is organized in the sections listed below. Section 2 talks about the important stages of the IoT Forensic process and the challenges faced in each stage. Section 3 gives a brief about Data Analytics before we move on to looking at IoT through the perspective of Data Analytics in Section 4. Section 5 mentions real-life cases from a legal forensics perspective and draws the parallels between IoT Forensics and Data Analytics in the cases solved by the authorities. Section 6 discusses the research gaps, limitations, and future scope of the paper, and Section 7 concludes the paper with our findings and the scope of improvements.

2 | MAJOR FORENSIC STEPS AND CHALLENGES FACED

Digital Forensics follows a certain order of steps to utilize the evidence in the best way towards concluding. IoT Forensics follows a similar set of steps as mentioned below [16]. Based on the Digital Evidence Life Cycle, the detailed steps can be seen in **FIGURE** 3 . Many factors, as shown in **FIGURE** 2 , affect IoT Forensics and the decision behind choosing the most appropriate source for a certain situation. Each step of the life cycle poses different challenges [17] in the domain of IoT Forensics.

2.1 | Identification

Search for and identifying the evidence is an essential part of any forensic examination, especially in IoT Forensics. Since the data is dispersed amongst cloud resources, individual network–attached storage units, or cryptocurrency wallets, among other

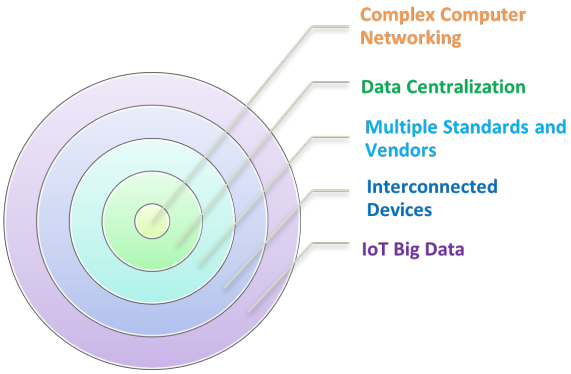

FIGURE 2 Factors affecting IoT Forensics

possible regions[16]. The Digital Forensic Examiners may not even know which device is compromised or where the physical data is. Further, even if the examiners know where the data is located, they might be unfamiliar with the type of IoT device and the components used. Legal issues regarding data protection and unauthorized intrusion may be another hindrance[16 18]. Hence, even the foremost step of the life cycle comes with challenges.

2.2 | Acquisition, Preservation, and Protection

Once the source of the evidence is identified, comes the issue of obtaining the evidence in the right way, termed "forensically sound manner" in the field of Digital Forensics[16]. It implies that a specific procedure must be applied while collecting the evidence information to make it usable in court. Further, data encryption can make it difficult to collect evidence. Once the data has been acquired in a forensically sound manner, another challenge is to be faced – preservation of the said data, keeping in mind the limited life span and memory space of most IoT devices, and guaranteeing its integrity, that is, guaranteeing that the data obtained is correct since data preserved in the cloud could have been changed or decrypted by a malicious user, and hence can be used as evidence efficiently[16]. Moreover, preserving the evidence alone isn't enough. It needs to be protected as well[19].

2.3 | Analysis and Correlation

IoT devices generate a large volume of data. Even after identifying the evidence from that data, a considerable amount is still to be analyzed. Such a large amount of further data points to a possible privacy issue since the data of a large amount of unintended and uninvolved users might be present as well, and their identity and privacy might be compromised[16 20]. In addition, the format in which the evidence was obtained has a great impact on the analysis. Further, correlating evidence from different IoT nodes is a challenging task since most IoT devices do not store any metadata[16]. Hence, this may lead to more speculation than logical proof and consistency behind the evidence.

2.4 | Documentation and Presentation

With the completion of the analysis, the challenges have ended, but that is not so. The documentation and presentation of the evidence require consideration of the legal systems, the jury involved, and the way the data should be presented to make the evidence and its reasoning clear[16].

3 | DATA ANALYTICS

Data Analytics is the science of analyzing raw data and making conclusions regarding the information[21]. It involves applying computer systems for analyzing large data sets to support decisions[21]. It involves various steps, from the problem statement, data collection, and data cleaning, to interpreting the results. **FIGURE** 4 shows the major steps of Data Analytics.

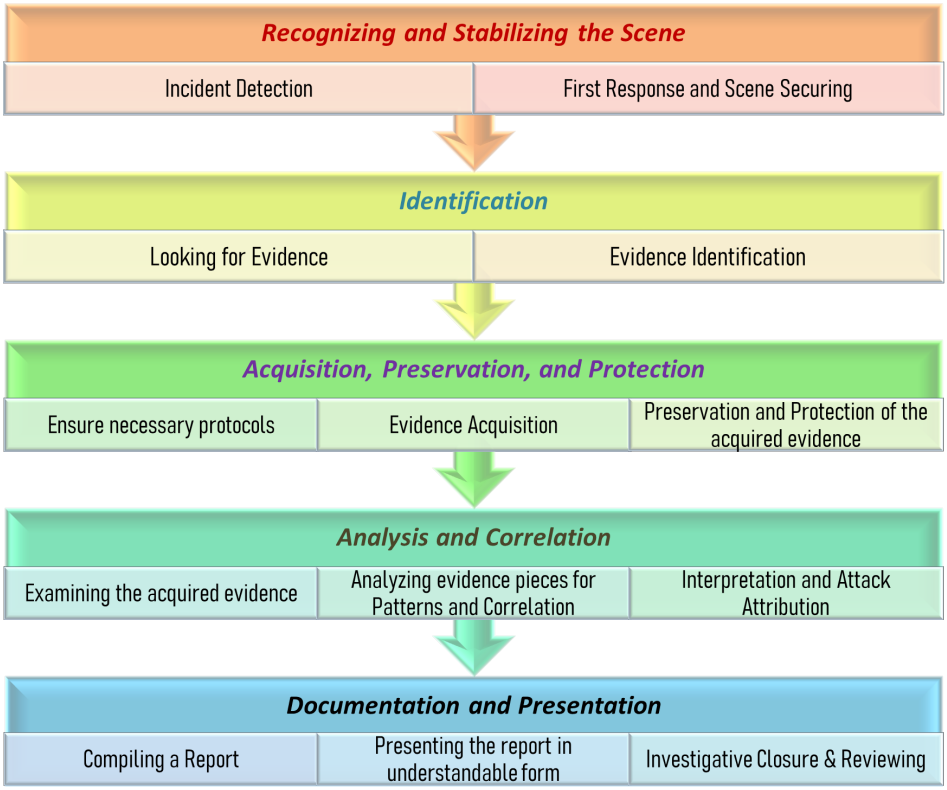

FIGURE 3 Digital Evidence Life Cycle

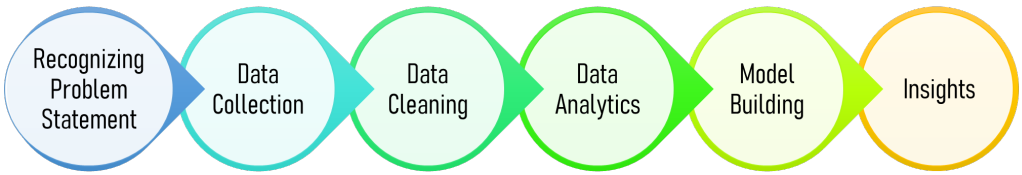

FIGURE 4 Major Steps of Data Analytics

3.1 | Types of Data Analytics

Data analytics can be broken into four basic types[22], namely:

- *Descriptive Analysis:* It looks for answers to *'What happened previously'* and provides insights into past events for comparison.
- *Diagnostic Analysis:* This analysis answers the *'Why did it happen'* question and helps in finding the cause behind the outcome shown from the insights gained from Descriptive Analysis.
- *Predictive Analysis:* This type analyses the data from past events and the causes to predict future outcomes, answering the *'What will happen next?'*
- *Prescriptive Analysis:* In this type of analysis, we answer the question of *'What should be done further?'* wherein the past decisions, causes, and outcomes are analyzed to estimate the likelihood of different outcomes.

The branch of Digital Forensics that involves identifying, obtaining, and analyzing digital evidence, present in the form of a large amount of data, from these IoT devices for legal or investigative purposes is termed IoT Forensics. It may even involve reconstructing a chain of events or a given crime scenario, applying investigative techniques, or even using post-mortem investigation. IoT Forensics is a time-restricted process that requires forensics readiness and falls under the judicial region that includes specification of legal aspects in legal service agreements regarding forensic issues.

4 | TAXONOMY OF IOT FORENSICS: FROM THE DATA ANALYTICS PERSPECTIVE

Traditional computers and forensics tools cannot keep up with the IoT domain's exponential data growth. The intricacy of the data may prevent investigators from conducting smooth data analysis in addition to the processing of a large volume of data. The typical "store-than-process" technique is no longer suitable for Big IoT forensic data, according to [23 24]. IoT Forensics techniques demand dynamic information processing using expandable analytics algorithms.

Based on the conventional steps of data analytics processes, it is required to identify the exact set of steps to be followed for analysis procedure in the IoT forensics scenarios. The logic of data analytics is required to be integrated with the forensics processes to be implemented on data acquired from various IoT devices. In other words, the steps involved in Data Analytics and IoT Forensics run in parallel. This is so because the 'evidence' talked of in IoT Forensics is initially nothing but raw data for most cases. A large amount of data available in the IoT devices, networks, and services is raw data before it undergoes the steps of Data Analytics and becomes valuable evidence, which is then analyzed, like processed data.

4.1 | Steps of Data Analytics for IoT Forensics

Some of the phases of IoT Forensics would require the same methodologies incorporated into Data Analytics, say, regression or classification of evidence, to conclude. Through this paper, we attempt to look through the world of IoT Forensics from the perspective of data analytics and what conclusion is reached upon applying said analytics in a forensically sound manner while analyzing the forensic evidence. At the same time, this article also provides a glimpse at the limitations brought forth while drawing the parallels.

FIGURE 5 shows the thematic taxonomy of data analytics solutions that can be designed for IoT forensics. These solutions are categorized based on the major functionalities involved in the analytics procedure for the forensics domain: A) Problem Statement Identification, B) Evidence Acquisition and Preservation, C) Analysis and Correlation, and D) Presentation.

4.1.1 | Identification of Problem Statement

The first step toward Data Analytics is to recognize the problem statement to decide what data to work upon. In any analytical situation, it is essential to realize what is to be worked upon to move further. As seen in the previous sections, similar is the case with IoT Forensics, where the 'evidence', which can be compared to the raw data in Data Analytics, is to be identified. There can be multiple sources and levels of sources present near the crime scene, but it is essential to identify what will eventually contribute as evidence. Therefore, considering the crime scene as the situation, identifying which devices, networks, or cloud storage to count under evidence is to be done through the problem statement realization.

4.1.2 | Acquisition & Preservation of Evidence

Once the problem statement has been identified; the data is collected and worked upon to convert it to a form that can be stored and analyzed. This falls under data collection and cleaning, where the latter is generally done through omissions or default additions. In the case of IoT Forensics, the evidence, once identified, is to be acquired to ensure the maintenance of unrelated users' security and privacy while acquiring the data. Once acquired, the evidence also needs to be preserved and protected. For this, the evidence must be shuffled through to remove any possible harmful files and to ensure that a small segment of misleading data does not corrupt the entire set of evidence.

4.1.3 | Analysis & Correlation

Once the data has been cleaned; it is to be analyzed to decide upon what model to build and to extract the statistics behind the problem statement. This analysis is done using various tools, from Excel to Redash and Power BI. The use of the tools

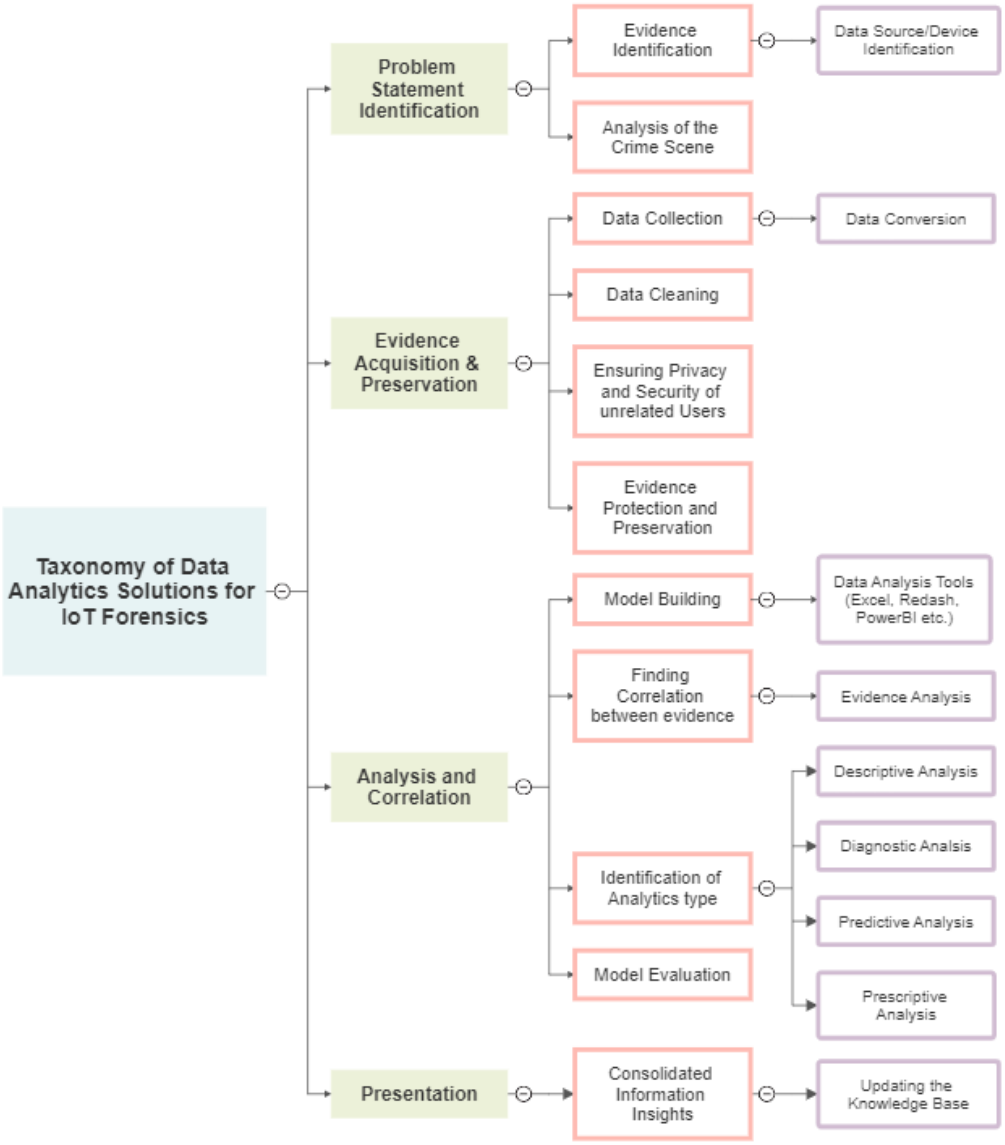

FIGURE 5 Taxonomy of Data Analytics Solutions for IoT Forensics

depends on the nature of the data to be analyzed and built upon. Once analyzed, the data is passed through the model to attain results relevant to the problem statement. Similarly, the preserved evidence of IoT Forensics is analyzed using various tools, again chosen depending on the data format, before a correlation can be set up between the different sets of evidence. Be it the correlation between suspect's answers and their proof of absence from the crime scene at the time of criminal activity or be it the correlation between a victim's messages and audio clip found through a smart device, it is through the evidence analysis that the authorities can shortlist the final set of evidence and correlate it.

It is particularly this phase of the two methodologies that draws up major parallels since the tools used for the analysis of evidence in IoT Forensics often match the analysis tools for Data Analytics, depending on the type of data or evidence preserved. Several file types might require using the same analysis techniques used in Data Analysis.

4.1.4 | Presentation

Once the analysis and model evaluation has churned out the results; these results are consolidated into information that can be understood by different sets of individuals and are used to attain information insights regarding the problem statement. These insights can be of use for both that situation, as well as for future similar situations as reference.

Correspondingly, for IoT Forensics, the evidence, once correlated to the final point, needs to be converted to a form that can be presented to the court in a format that can be understood by different sets of individuals, including ones who are not well versed with technical terms. Further, it must be documented to be of value to the current case, as well as to be of reference to future plausible similar cases.

4.2 | Data Sources in IoT Forensics

It is crucial to identify the sources of data collection that can later be used as evidence in IoT forensics scenarios. The data stored in different IoT devices present at the investigation scene can provide valuable information for forensic processes. The following text describes how various data sources can play a vital role in extracting evidence.

In the majority of intelligent home setups, devices of different kinds may connect to a hub and transmit interaction data, temperature or moisture data, and other relevant data. Humidity, temperature, motion, etc., parameters can observe changes as an event occurs, giving us a plethora of information about it. Data stored in device applications, local networks, cloud-based logs, and metadata about different actions can all serve as proof to show what connected individuals and devices have been doing.

TABLE 2 Evidence/Data Sources in different Forensic Scenarios

Forensic Scenarios	Object of Investigation	Evidence Sources
A residential house equipped with different smart/automated devices	Smart Home	Apps installed in victims' phones/computers for smart appliances; Data stored in smart appliances; Data stored on the cloud through various apps for smart devices; Activity log for local networks; Smart Hub;
An incident involving one or more intelligent automobiles	Smart Vehicles	Logs of vehicle-network communication; GPS systems; In-built vehicle sensors; Advanced applications installed in automobiles; Automotive networks; Traffic cameras/sensors controlled by local authorities
Victims or suspects or witnesses wearing smart healthcare devices	Smart Wearables	Smartwatches/ smart glasses, smart rings, implants, AR glasses, VR headsets, smart shoes; Applications installed on smartphones/PCs; Devic communication logs; Data stored on cloud
Presence of IoT/controlling devices at the investigation scene	IoT-enabled devices	Computer storage; Web applications; Browser history; Field devices; Client applications; Server/system logs; Network traffic patterns

For collecting evidence related to different types of automotive, we can usually focus on the vehicles' in-built features for safety and convenience, including telematics and various sensors for parking assistance and gaining knowledge of the surroundings[25]. Due to such advanced automotive features, smart vehicles can act as a repository of evidence. Certain vehicles also have advanced sensors, such as seat occupancy sensors and hands-free phone systems, which can be used to identify the driver or passengers. Moreover, using GPS systems, it becomes easy to find a trail of past locations visited by the vehicle.

Data stored in devices and data moving over networks are the two main forms of evidence in control systems. However, the evidence-acquisition process may face difficulties because of the diversity in control system components. Data acquisition from field devices, such as smart meters, programmable logic controllers, and phasor measurement units, may not be done directly as it is required to run memory imaging code on the control system first. Memory dumps can also be used to recover objects, including data files, network logs, login information, and server synchronization statistics. Potentially admissible information can be obtained from a variety of wearable devices. Evidence acquisition from such devices includes geolocation data, user profiles, health data, activity logs, social media account information, calendar information, media files, and usage patterns.

When it comes to forensic situations in the IoT context, such as those involving household appliances, medical equipment, and networked automobiles, the evidence sources alter significantly[26]. **TABLE**2 provides a summary of the primary sources of data to be used as evidence in the major IoT forensics scenarios.

4.3 | Challenges in the implementation of Data Analytics for IoT Forensics

Due to the complexity and crucial requirements of the forensic processes, it isn't easy to integrate the concepts of Data Analytics for IoT Forensics. Some major challenges in this regard are discussed below:

i) *High Performance Computing for Data Processing*
The rise in cybersecurity threats has introduced the need for developing more efficient and cost-effective solutions for forensics processes[27]. However, as discussed in[28], the current digital forensic techniques' computational power is insufficient for most forensic investigation cases. The leading causes are the unavailability of clear performance criteria and indicators and giving more weightage to accuracy than the overall process efficiency. Therefore, high-performance computing can be an excellent choice in such scenarios to improve processing times and overall performance as it significantly reduces processing time during data/evidence processing, evaluation, and presentation phases.

ii) *Error Analysis*
In forensics, detecting errors and countermeasures required for correcting them revolves around testing and validation processes. The basic objective of analyzing errors in IoT forensics is to assess all possible human or technical error sources. Techniques are to be developed to take preventive measures and lower the likelihood of future erroneous conditions. The key requirement is that such techniques should not exhibit any biased behavior for any user or computer algorithms during the analysis process.

iii) *Data Exclusion/Inclusion*
Any forensics investigation should be initiated with data collection. However, not every piece of data that is gathered and examined could or should be included in the evidentiary assessment[29]. The assessing team must establish and enforce precise inclusion/exclusion guidelines to ascertain what data is pertinent and what is not. The left-out information is also required to be preserved. The timeframe for preserving such information should be determined based on standard legal practices. It is also important to safeguard this information; hence, the storage facility should be designed according to this requirement.

iv) *Process Automation through Artificial Intelligence*
The implementation of computer intelligence strategies such as machine learning, artificial intelligence, and deep learning in the forensics domain has been of great interest since the beginning[30]. Over the years, numerous efforts have been made for intrusion and anomaly detection/classification, rule mining and forensic multimedia analysis, etc.[31 32 33 34]. The major advantage of automating forensic processes is a significant reduction in processing time, efforts, and cost associated with forensic investigations[35]. It improves the correctness and accuracy of the outcome to a great extent by lowering human errors. Automation is quite important when the investigation involves a large volume of evidence data beyond human experts' capacity to deal with it. Along with the benefits mentioned above, intelligent automation of forensic processes, especially data analytics processes, impose some important concerns. According to[3], the reliability of automated processes might affect the caliber of forensic experts. Also, there are possible scenarios in a forensic investigation that need human insights and intuition, especially for identifying and correlating the potential evidence. Moreover, current data processing techniques are facing some challenges when applied to the digital forensics field[36]. Also, the risk of evidence omission and the possibility of missing some of the numerous IoT devices placed in various locations cannot be ignored.

v) *Big Data Analytics*
The main limitation of conventional computers and forensics tools is that they can't keep up with the exponential growth in the data produced by numerous IoT devices for evidence acquisition and processing purposes. Apart from the challenge of dealing with a large volume of data, another major difficulty is implementing smooth data analytics due to the complexity of information. The typical "store-then-process" technique is no longer suitable for Big IoT forensic data[10]. The IoT Forensics techniques must be backed by reactive data processing and analytics techniques that also exhibit high scalability.

vi) *Data Reduction*
To handle the enormous amount of forensic data in a time-constrained environment, it is necessary to reduce the amount of data and its processing. This can be achieved through selective redundancy, and optimal data extraction methodologies[37]. Great care should be taken while scaling back the amount of forensic data as it is very important to retain the original formats, attributes, and aspects for voluminous real-time IoT data sets.

vii) *Cross-device Analysis*
As described in[36] and[37], forensics methods and tools are available for assessing numerous data subsets and identifying connections between data stored in the cloud, disks, and portable devices. Different feature extraction techniques are useful for identifying unique parameters in potential evidentiary data. It is needed to lower the analysis time. It acquires deeper knowledge about the incidents by extending the search process to incorporate different devices and integrating data from several heterogeneous sources.

viii) *Privacy Preservation*
It is crucial to maintain privacy while analyzing data from various IoT devices and other sources. The main reason for protecting privacy is that such data sources contain confidential information about the user and his activities. Not every piece of such information is required for forensic analysis. Accessing non-relevant, private information might lead the investigators to build biased assumptions and can deviate the assessment process from the original motivation. Therefore, striking the right balance between gathering crucial evidence and preserving user privacy is challenging. Latest encryption techniques pose new difficulties for forensic processes as most support end-to-end encryption and storing confidential data on the cloud or servers. Hence, it cannot be obtained without the involvement of service providers.

TABLE3 highlights the major requirements and challenges in implementing the data analytics phases and their processes when the same is to be applied in the IoT forensics domain.

5 | RECENT CASE STUDIES ON IOT FORENSICS

To analyze the parallels and possible differences between IoT Forensics and Data Analytics, as mentioned in the previous section, six solved IoT Forensics-based case studies have been approached below[9]. Two of the case studies have been taken from the webpage of Law and Forensics[9], a global legal engineering firm. The other case studies[38] have been drawn from different incidents featured in news articles open to the public. So, while the first two cases are examples of how well drawn out the steps of IoT Forensics and Data Analytics are, the other cases are from a time when IoT Forensics was a novel concept and didn't include a certain set of rules or steps for investigation. These are cases where IoT technologies weren't the focus of the investigation; rather, they have been the silent witnesses. These cases are described in brief in this section. All the cases have been summarized with the relevant details in **TABLE**4 . This table also shows the sources of evidence for IoT Forensics, how this evidence is identified and acquired, how relevant data is extracted from the collected evidence, what level of IoT forensics is applied, and whether the standard Data Analytics processes were used during the investigation process.

5.1 | Medical Device Manufacturing Case

In this, the law firm assisted a national medical device manufacturing firm in performing forensics on various IoT devices as part of an internal investigation related to the Whistleblower, and Qui Tam litigations[9]. In this lawsuit, the government was claimed of being scammed in the healthcare, pharmaceutical, and medical instruments industries. Federal and state governments spend trillions of dollars annually on prescribed medications, surgical instruments, hospitalization, ambulatory care, doctor appointments, and assisted living facilities through Medicare and other government healthcare-support programs. The government depends on individuals and companies to uphold the law and provide proper compensation claims to reimburse such services. However, some businesses and people disregard this and submit fake or fraudulent reimbursement claims.

- Here, first, the problem statement was recognized, which involved understanding what devices, networks, or cloud forensics might help the investigation regarding the Whistleblower of Qui Tam litigation.

TABLE 3 Challenges in the Implementation of Data Analytics phases for IoT Forensics

Requirements	Mapping with Data Analytics Phases for IoT Forensics	Challenges
High-Performance Data Processing	• Data Processing • Analysis and Correlation • Presentation	Existing computational power is not sufficient for forensic computations; Need for efficient computing methods that focus on performance, accuracy, and cost
Error Analysis	• Analysis and Correlation • Model Building	Standardizing methods for analyzing all possible human or technical errors; Ensuring unbiased error analysis
Data Inclusion/ Data Exclusion	• Data/Evidence Acquisition and Preservation • Data Cleaning	Determining what to include or exclude during the evidentiary assessment; Preservation of excluded information abiding forensics laws and regulations
Analytics Automation	• Data Cleaning • Analysis and Correlation • Model Building	Finding appropriate techniques for automating forensic data analytics processes through artificial intelligence; Over-reliance on automation; Lack of human intuition during a forensic investigation
Big Data Analytics	• Data/Evidence Acquisition and Preservation • Analysis and Correlation • Model Building	Typical "Store-then-process" is not applicable to big IoT data; Need for highly scalable and efficient data processing and analysis techniques
Data Reduction	• Data/Evidence Acquisition and Preservation • Data Cleaning	Handling of an enormous amount of evidence data in a time-constrained environment; Retaining original data formats and metadata
Cross-device Analysis	• Evidence Identification • Data/Evidence Acquisition and Preservation • Data Processing • Analysis and Correlation	Identification of linkages between data subsets stored across various storage media; Search algorithms should run through heterogeneous data sources and dissimilar IoT devices
Privacy Preservation	• Evidence Identification • Data/Evidence Acquisition and Preservation • Model Building • Presentation	Private, irrelevant user data should not be accessible to investigators to maintain confidentiality and unbiased assessment; Service providers' intervention is unavoidable in most cases; Difficult to obtain evidence in un-encrypted forms

- Once identified the (data) evidence had to be collected from different sources, particularly IoT devices. This data collected (acquired) from different IoT devices, hard drives, and backup tapes had to be converted to a preservable format and then protected from malicious attackers who might disrupt the case. For preservation purposes, the data (evidence) cleaning involved dealing with several deleted, hidden, lost, possibly corrupted, and encrypted files[9]. Once the evidence had been collected and cleaned, it had to be protected forensically sound.

- This data, once protected, was then analyzed and correlated to match witness and employee statements. To match the audio, several files had to be analyzed through speech recognition tools.
- Once the final set of evidence was shortlisted, the firm officials confirmed the final list of perpetrators. The entire case was documented in a format understandable by law officials and then handed over to the respective authorities. The insights from the case were documented to be useful for similar Whistleblower litigation cases in the future.

5.2 | Pharmaceutical Sector Case

In this, the firm had been hired by an outside law firm for the conduction of a foreign investigation as part of a trade secret and economic espionage dispute with a competitor in the pharmaceutical sector[9].

- Here, initially, the problem statement was recognized, which involved understanding what devices, networks, or cloud forensics might help the investigation regarding economic espionage and trade secret litigation.
- Once identified the (data) evidence had to be collected from different sources. In this scenario, many servers (network) and cloud-level sources of IoT were also involved. This data which was collected (acquired) from various devices, computers, servers, and cloud storage, had to be transformed into a preservable format – alongside the large-scale interviews of various company engineers and then protected from the possible attacks of the other party. The evidence acquisition was a sensitive step that involved the exfiltration of 1200 confidential files. For preservation, these files had to be decrypted in a secure environment. Once the evidence had been collected and cleaned, it had to be protected forensically sound.
- The next step for the firm was to analyze the data and match the proof to break the case in favor of their client. Since the case involved trade secrets, certain vital terms were correlated, using data analysis models, amongst the files and communications to find proof of trade secret litigation.
- Once the solid proof was available, the firm officials drafted and submitted an expert report in a format understandable by law officials. They then presented the report to the court to win the case in favor of their client. The insights from the case, particularly the tricky extraction of confidential files through IoT devices, could be of great value to any such trade secret litigation cases in the future.

5.3 | Dabate Fitbit Murder Case

In this incident, on December 23, 2015, a man named Richard Dabate reported his wife Connie's murder while stating that there had been an attack from a masked intruder. According to Richard's initial statement to the police, he had gone to work after dropping off the kids on the bus, and soon after, his wife had gone for a fitness class at the local YMCA. However, Richard soon noticed that he had forgotten his laptop, and upon returning home between 8:45 am and 9:00 am to get back the device, he decided to check a noise he had heard upstairs. There, he encountered the intruder. According to Richard's narrative, the events post the encounter went in this order: just when he noticed the intruder, his wife returned home. Dabate yelled a warning to his wife and asked her to run, but the intruder shot the wife, killing her. Post this; he mentioned that the intruder half-tied him to the chair and tried burning him, but he struggled and turned the torch on the intruder. In response, the intruder dropped the torch and ran out while covering his face with his hands. Once he left, Richard crawled upstairs with the chair attached to his wrist, pushed the panic button on the house alarm, and called 911[39].

- Here, firstly, the problem statement was recognized which, for the investigation officers, was finding proof behind Richard's statement regarding his wife's murder. This involved collecting all the evidence involved. Unlike the previous cases, the priority here wasn't collecting evidence from IoT devices, networks, or the cloud. Rather, the authorities first tried finding signs of intrusion, forced entry, and the presence of an intruder, alongside trying to find other evidence. The latter included Connie's Fitbit (the IoT device), the husband and wife's phones, computers, and the house alarm logs (IoT-based sensors).
- Once they identified the evidence, the authorities registered a search warrant to look through the data and alarm logs. Once the warrant was acquired and the evidence obtained, the logs were handled carefully to ensure no data was deleted or corrupted by any parties involved.

- This data (evidence) was studied manually to check a match for the time and distance of Connie Dabate's movements to Richard's statements. The house logs showed that Richard had logged onto Outlook from the IP address assigned to his house internet, from where he sent an e-mail to his supervisor (around 9:04 am) that he had to return home to check an alarm that had gone off. This did not match his statement to the police about accidentally leaving the laptop at home. Next, Connie's Fitbit data was checked. The data were filtered (cleaned) through to directly focus on the time when Connie entered the house around 9:23 am and this was matched with the house logs registering that the garage door had opened into the kitchen. Between 9:40 and 9:46 am, the house IP address was used by Connie for browsing Facebook and uploading videos on her page. From when she entered the house to nearly 10:05 am, about 1217 feet of distance was logged into the Fitbit before her movement stopped, and the Fitbit registered an improper heart rate. According to the news report, if Richard's statements were to be correlated to this data, her movement would be about 125 feet at the most.

- Once the evidence was stacked up, the police gathered insights and charged Richard Dabate with murder, tampering with physical evidence, and false statements. When brought up in court, many different steps were to be taken, such as proving the accuracy of Fitbit before the evidence was considered presentable in the court. The case is still ongoing and has seen delays due to COVID-19.

- As mentioned before, unlike the previous two case studies, this case isn't one that focused on IoT Forensics from the beginning. The focus on this case was slightly different. Hence, rather than the involvement of forensic experts from the very beginning, only the local police were involved at first. Further, most data had to be manually matched with the statements. Had a Data Analytics model been available, it would have been easier to find the discrepancies between the statement, the logs directly, and the Fitbit records to obtain the results.

5.4 | Karen Navarra Murder Case

Karen Navarra, 67, was murdered on September 8, 2018, and her body was discovered, in her house, five days later[40]. The authorities found her dead on the scene upon receiving a call from a co-worker who had visited the house after the victim failed to show up to work, with a gaping wound to her neck and several wounds on the top of her head. A large kitchen knife was found in her right hand, which according to the police reports, was done to stage the murder as a suicide. Through several on-scene evidence pieces, it was clear that it was a murder case rather than a staged suicide. However, it wasn't until they utilized technology, particularly IoT-based evidence, that they could charge the victim's stepfather, Anthony Aiello, with murder.

- Here, the initial problem statement for the investigators was to confirm whether the case was one of a suicide or murder. To confirm the same, they looked through the on-scene evidence in the form of body position, the hand holding the knife, the position of the stab wound, and other such pieces of evidence. Post that came to the main problem statement for the authorities: to identify the murderer. For this, they took the help of technology.

- The initial evidence identification involved looking for evidence at the scene of the crime. Post that, the technological evidence provided a breakthrough for the authorities. These included video surveillance and the victim's Fitbit data.

- The initial evidence acquisition involved checking the video surveillance, through which it was observed that the victim's 90-year-old stepfather, Anthony Aiello, had visited the victim on the day of her death. The suspect was arrested on September 25. However, the suspect claimed he had been there to drop off food for his stepdaughter and had left the house within 15 minutes. Further, he also said that he saw the victim drive by his home later that afternoon. Alongside the video surveillance, the police got a search warrant for the Fitbit data of the victim. Once this was granted to them, aided by Fitbit's brand protection director, the data was compared to that of the video surveillance. Now, one important point to note is that the data was only provided to the authorities after it had been cleared according to the privacy policy of the Fitbit company. The company also published a copy of its policy in the New York Times, stating that it complied with the legal processes – both the search warrants and the court orders while sharing the data.

- Once the evidence had been retrieved, the pieces of evidence were analyzed. The suspect's statement that he was only at the victim's house for 15 minutes did not match, as the surveillance showed his car to be parked outside the victim's house for at least 21 minutes. Further, according to the suspect's statement, he had seen the victim driving past his home with someone later the same day. However, based on the video surveillance, the victim's car never left the house that day. Another piece of evidence instrumental in the arrest was the heart rate data of the victim as registered by Fitbit. According

to the data, the victim's heart rate had spiked significantly at 6:20 pm EDT, followed by a rapid fall in the rate and an eventual stop at 6:28 pm EDT. This matched with the 21 minutes – from 6:12 pm EDT to 6:33 pm EDT, during which her stepfather, the suspect, was in her house[41]. When confronted about the same, the suspect insisted that there must have been someone else in the house, which contradicted his initial statement that he hadn't seen anyone else in Navarra's house when he left. These pieces, along with other external plausible evidence amongst the perpetrator's belongings, led to his arrest.

- The evidence was compiled and presented to a grand jury that indicted Aiello on August 7, 2019. This case shows how data collected from IoT Forensics can prove circumstantial evidence for the case. Without the Fitbit data, the suspect was disadvantaged due to the mismatch between his statements and the video evidence. However, it might have been ruled as insufficient evidence. The IoT data collected and analyzed, with its analysis aided by Fitbit's director of brand protection, was the final key to connecting the perpetrator to the case. Hence, it also shows that when legal processes are involved properly alongside data analytics, it becomes a strength for the authorities involved.

5.5 | 2017 Hit and Murder Case

This case was initially pursued by the Prosecutors and the police with a charge of "death by dangerous driving" before being elevated to murder after evidence from vehicle infotainment, and telematics surfaced. On August 5, 2017, the accused and others got into an altercation at the bar with the victim and his friend. The altercation moved outside, and the 18-year-old victim Soban Khan threw a bottle, which damaged the side view mirror of a red Ford Mustang, belonging to the guilty[42 43]. The drunk 24-year-old flew into a rage and chased Soban and his friend, who had fled on a moped. Had it not been for the data stored in the vehicles, the case might have been an accidental death while trying to confront. However, evidence suggested otherwise. Looking into the steps in detail, it shall be evident how IoT Forensics, even as just a sub-part of the investigation, played an important role.

- The police recognized the problem statement as finding proof of the altercation, collision, and death of Soban due to the collision of the Mustang and the moped. While the main objective hadn't disclosed the result, looking through the data in the vehicle systems was a crucial part of the objective.
- The authorities collected statements from witnesses, evidence from the closed-circuit camera, and forensics from the vehicles and the crime scene. The evidence was carefully collected in a forensically sound manner. To ensure evidence maintenance before analysis, the forensics were sent for preservation.
- In this case, the statements from the witnesses differed, and there were gaps in the evidence gathered from the cameras. So, the authorities had to rely heavily on the evidence from the scene and the data available in the vehicles. The damage on the scene brought up the charges of "death by dangerous driving." However, when the vehicle data was accessed and drawn up to the model to relate the speed to the evidence gathered, it was observed that the car acceleration was too high for a simple angry chase. Also, it was observed that when it approached the moped, it simply increased at the moment of the impact. Additional data on the systems also showed that the driver intended to mow down the two people on the moped. Further, there was evidence that even after the collision, the driver leaped out of the vehicle and continued beating the victim, pronounced dead on the scene around an hour and a half after the crash.
- Based on the vehicle systems evidence, conclusions were drawn, and the charges were elevated to murder. The evidence was presented to the jury, who later convicted him of murder and attempted to conflict grievous bodily harm.
- In this case, the presence of IoT Forensics was essential in bringing out a clearer picture of the crime scene and the crime itself. As a result, justice was served better with the help of IoT Forensics. Data Analytics comes into the picture here, particularly while comparing the acceleration speed[44]. Had better Data Analytics techniques been employed alongside the forensics from the beginning, it might have been easier to predict the events preceding the collision.

5.6 | Ross Compton Arson Case

This case is to highlight the limitations that come alongside IoT Forensics, particularly from the legal aspects. In this case, Ross Compton, whose house had caught fire, answered the police that he'd been sleeping when the fire started and when he

TABLE 4 Analysis of Case Studies

Case	Case Type	Category of IoT Forensics	IoT Device used as Evidence	Phases of Data Analytics/IoT Forensics Applied	Remarks
Medical Device Manufacturing Case[9]	Litigations regarding fake healthcare claims	Device, Network, and Cloud-level Forensics	Data collected directly from various IoT devices, hard drives, backup tapes as well as from cloud storage	Problem Statement Identification, Evidence Acquisition, and Preservation, Analysis and Correlation, Presentation	Well-implemented steps of IoT Forensics and Data Analytics
Pharmaceutical Sector Case[9]	Trade Secret and Economic Espionage Dispute	Device, Network, and Cloud-level Forensics	Data collected from servers, cloud storage, IoT devices, and computers to extract more than 1200 files	Problem Statement Identification, Evidence Acquisition, and Preservation, Analysis, and Correlation, Presentation	Well-implemented steps of IoT Forensics and Data Analytics
Dabate Fitbit Murder Case[39]	Murder on Residential Premises	Device-level Forensics (The Fitbit) and Network-level Forensics (alarm logs)	Mobile phones, computers, alarm logs, and smartwatch data	Partial evidence acquisition through IoT devices; manual evaluation and analysis of evidence without following the standard rules/processes of data analytics	Didn't apply the steps of IoT Forensics/Data Analytics; IoT technology was just a silent witness during the investigation
Karen Navarra Murder Case[40]	Murder by hitting and stabbing	Device and Network-level Forensics	Victim's Fitbit data and video surveillance	Problem statement identification, manual evidence identification, and acquisition, manual analysis of evidence data	Used IoT Forensics to collect evidence; Applied a few steps of data analytics to process the evidence
Hit and Murder Case[42]	Hit and Murder	Device-level Forensics	Vehicle data, and telematics	Problem statement identification, evidence acquisition/preservation, partial data analysis	IoT Forensics helped to identify the case as an intentional murder and not an accident; Proper use of Data Analytics could've made the investigation process much easier and faster
Ross Compton Arson Case[45]	Arson Case	Device-level Forensics	Pacemaker Data	Evidence acquisition, data cleaning, analysis, and correlation	IoT Forensics and Data Analytics helped to identify the case as an arson attempt, not an accident; Raised the issue of protecting the accused's private data on legal grounds

woke up, on seeing the fire, he immediately packed some belongings, broke the glass of his bedroom window with a cane, threw his belongings out of the window before climbing down himself and carrying them over to his car[45].

- When the police arrived, their focus was to find the reason behind the fire, whether it was accidental or a deliberate arson attempt. Initially unsure of what to consider as evidence, they started by questioning Compton, who mentioned that he had a cardiac pacemaker.
- The police found that the fire had started from multiple locations in the house and that there were traces of gasoline on Compton's clothing. This prompted the authorities to request a search warrant to retrieve the electronic records stored in the heart device. Once the warrant was approved, they obtained data regarding Ross Compton's heart rate, pacer demand, and cardiac rhythms before, during, and after the fire. This data was cleaned and focused on the duration of the incident.
- The data from the pacemaker was analyzed and correlated to the probable heart rate that would have been in case Compton did all the steps mentioned in his statement, and it was found that, given his condition, it was highly improbable for Compton to have heaved the collected, heaved, and then thrown the luggage down the window, in such a short time, without increasing the pacemaker rate too much higher levels.

- Based on the analysis, the police logged the charges of arson against Compton and presented the case to the jury. His attorneys appealed, however, to the 12th District Court of Appeal that the use of the medical records involved physician-patient privilege and a decision had to be taken before the trial on whether the use of pacemaker data and the issuing of a search warrant for the same could be allowed[46].
- This case study brings forth the questions of legality that need to be ensured in any forensic methodology, even IoT Forensics. Further, analyzing the evidence obtained needs an even clearer protocol set to solidify the case in court.

6 | RESEARCH GAPS, LIMITATIONS, AND FUTURE SCOPE

IoT Forensics is a domain yet to be explored thoroughly. It has gained some recognition in the past few years as seen by existing literature such as[47], but there is still much to be researched. Keeping this in mind, it took more work to find existing literature that tallies IoT Forensics in terms of Data Analytics and looks at IoT Forensics through the lens of data. Literature review on IoT Forensics majorly turned up material on IoT Forensics in general, it's understanding in terms of Digital Forensics, its approaches, and the challenges faced during the process of IoT Forensics.

Hence, while this paper talks of IoT Forensics from the perspective of Data Analytics, there is little physical implementation and very few prevailing statistics to base the comparisons upon. Further, this paper focuses majorly on IoT Forensics from the outlook of Data Analytics and evidence from the viewpoint of data. However, while evidence is in its essence, like the data from Data Analytics, it is more subjective and involves the human variant, which makes it more easily comprised. Data, on the other hand, generally involves categorical or quantitative variables. Moreover, Data Analytics is more accurate in providing general insights rather than a single outcome. In cases where a single perpetrator is to be found, Data Analytics can only be useful to a certain extent. The rest involves human intervention and moderation. Moreover, before incorporating it into Forensics completely, there needs to be an established protocol set regarding the methods employed in various stages of Data Analytics, as is currently a challenge of IoT Forensics[48].

7 | CONCLUSION

IoT is a domain that has thoroughly integrated into most people's lives and shall prevail as an interdisciplinary field in the upcoming years. This makes IoT devices, networks, and clouds an essential part of crime scenes, bringing in the field of IoT Forensics, a special branch of Digital Forensics that handles the evidence collected from IoT sources. This set of evidence generally involves the steps and process of Data Analytics in most of its evidence life cycle. This brings in the main purpose of this paper, which was to interpret IoT Forensics in the content of Data Analytics, and comparing the two, develop an understanding of whether Data Analytics can be incorporated into Forensics by itself. While we concluded that at its current standing, Data Analytics could, at most, run certain parallels with IoT Forensics. Eventually, it may be possible to integrate it into IoT and Digital Forensics, with as little human intervention as possible, given that certain protocols and external factors are considered thoroughly.

DATA AVAILABILITY STATEMENT

There is no data available to carry out this research.

CONFLICT OF INTEREST

Authors want to declare that at the time of submission of this article there is no conflict of Interest.

References

1. Khanpara P, Lavingia K, Trivedi R, Tanwar S, Verma A, Sharma R. A context-aware internet of things-driven security scheme for smart homes. *Security and Privacy*: e269.
2. Anand P, Singh Y, Selwal A, Alazab M, Tanwar S, Kumar N. IoT Vulnerability Assessment for Sustainable Computing: Threats, Current Solutions, and Open Challenges. *IEEE Access* 2020; 8: 168825-168853. doi: 10.1109/ACCESS.2020.3022842
3. Trivedi R, Khanpara P. Robust and secure routing protocols for MANET-based internet of things systems—A survey. In: Springer. 2021 (pp. 175–188).
4. Khanpara P, Trivedi B. Security in mobile ad hoc networks. In: Proceedings of International Conference on Communication and Networks. ; 2017: 501–511.
5. MacDermott A, Baker T, Shi Q. Iot forensics: Challenges for the ioa era. In: 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS). ; 2018: 1–5.
6. Prasad VK, Bhavsar MD, Tanwar S. Influence of Montoring: Fog and Edge Computing. *Scalable Comput. Pract. Exp.* 2019; 20: 365-376.
7. Khanpara P, Tanwar S. Additive manufacturing: concepts and technologies. In: Springer. 2020 (pp. 171–185).
8. Stoyanova M, Nikoloudakis Y, Panagiotakis S, Pallis E, Markakis EK. A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials* 2020; 22(2): 1191–1221.
9. Internet of Things (IoT) Forensics, Law and Forensics. https://www.lawandforensics.com/forensic-services/internet-of-things-forensics-2/, note = Accessed: Nov 18, 2022; .
10. Yaqoob I, Hashem IAT, Ahmed A, Kazmi SA, Hong CS. Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. *Future Generation Computer Systems* 2019; 92: 265–275.
11. Dunn R. IoT Applications in Forensics. https://www.iotforall.com/iot-applications-forensics/, note = Accessed: Oct 10, 2022; .
12. Alenezi A, Atlam H, Alsagri R, Alassafi M, Wills G. IoT forensics: A state-of-the-art review, callenges and future directions. 2019.
13. Shah M, Khanpara P. Survey of techniques used for tolerance of flooding attacks in DTN. In: Springer. 2019 (pp. 599–607).
14. Surange G, Khatri P. Integrated intelligent IOT forensic framework for data acquisition through open-source tools. *International Journal of Information Technology* 2022; 14(6): 3011–3018.
15. Gupta R, Thakker U, Tanwar S, Obaidat MS, Hsiao KF. BITS: A Blockchain-driven Intelligent Scheme for Telesurgery System. In: 2020 International Conference on Computer, Information and Telecommunication Systems (CITS). ; 2020: 1-5
16. Joseph MA. Digital Forensics is ready for its most recent challenge: IoT Forensics. https://www.linkedin.com/pulse/digital-forensics-ready-its-most-recent-challenge-iot-joseph/, note = Accessed: Sep 6, 2022; .
17. Conti M, Dehghantanha A, Franke K, Watson S. Internet of Things security and forensics: Challenges and opportunities. 2018.
18. Sandvik JP, Franke K, Abie H, Årnes A. Quantifying data volatility for IoT forensics with examples from Contiki OS. *Forensic Science International: Digital Investigation* 2022; 40: 301343.
19. Rughani PH. IoT evidence acquisition—Issues and challenges. *Advances in Computational Sciences and Technology* 2017; 10(5): 1285–1293.
20. Atlam HF, Hemdan EED, Alenezi A, Alassafi MO, Wills GB. Internet of things forensics: A review. *Internet of Things* 2020; 11: 100220.

21. Runkler TA. *Data analytics*. Springer . 2020.

22. J. Frankenfield AD, Rathburn P. Data Analytics. https://www.investopedia.com/terms/d/data-analytics.asp/, note = Accessed: Sep 8, 2022; .

23. Khanpara P, Lavingia K. Energy conservation in multimedia big data computing and the Internet of Things—A challenge. In: Springer. 2020 (pp. 37–57).

24. Khalid Alabdulsalam S, Duong TQ, Raymond Choo KK, Le-Khac NA. An efficient IoT forensic approach for the evidence acquisition and analysis based on network link. *Logic Journal of the IGPL* 2022.

25. Tanwar S, Tyagi S, Budhiraja I, Kumar N. Tactile Internet for Autonomous Vehicles: Latency and Reliability Analysis. *IEEE Wireless Communications* 2019; 26(4): 66-72. doi: 10.1109/MWC.2019.1800553

26. Kumar A. Data Analytics: Step by Step Approach, Medium. https://medium.datadriveninvestor.com/data-analytics-step-by-step-approach-757c6a0bd8a2/, note = Accessed: Sep 8, 2022; .

27. Rana N, Sansanwal G, Khatter K, Singh S. Taxonomy of digital forensics: Investigation tools and challenges. *arXiv preprint arXiv:1709.06529* 2017.

28. Lillis D, Becker B, O'Sullivan T, Scanlon M. Current challenges and future research areas for digital forensic investigation. *arXiv preprint arXiv:1604.03850* 2016.

29. Karie NM, Kebande VR, Venter H, Choo KKR. On the importance of standardising the process of generating digital forensic reports. *Forensic Science International: Reports* 2019; 1: 100008.

30. Patel K, Mehta D, Mistry C, et al. Facial Sentiment Analysis Using AI Techniques: State-of-the-Art, Taxonomies, and Challenges. *IEEE Access* 2020; 8: 90495-90519. doi: 10.1109/ACCESS.2020.2993803

31. Xiao J, Li S, Xu Q. Video-based evidence analysis and extraction in digital forensic investigation. *IEEE Access* 2019; 7: 55432–55442.

32. Shalaginov A, Franke K. Big data analytics by automated generation of fuzzy rules for Network Forensics Readiness. *Applied Soft Computing* 2017; 52: 359–375.

33. Krivchenkov A, Misnevs B, Pavlyuk D. Intelligent methods in digital forensics: state of the art. In: International Conference on Reliability and Statistics in Transportation and Communication. ; 2018: 274–284.

34. Buczak AL, Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications surveys & tutorials* 2015; 18(2): 1153–1176.

35. Caviglione L, Wendzel S, Mazurczyk W. The future of digital forensics: Challenges and the road ahead. *IEEE Security & Privacy* 2017; 15(6): 12–17.

36. Vincze EA. Challenges in digital forensics. *Police Practice and Research* 2016; 17(2): 183–194.

37. Quick D, Choo KKR. IoT device forensics and data reduction. *IEEE Access* 2018; 6: 47566–47574.

38. Murali J. Internet of Things based crime investigation. https://www.deccanchronicle.com/nation/current-affairs/220419/internet-of-things-based-crime-investigation.html/, note = Accessed: Sep 8, 2022; .

39. Watts A. Cops use murdered woman's Fitbit to charge her husband, CNN. https://edition.cnn.com/2017/04/25/us/fitbit-womans-death-investigation-trnd/index.html/, note = Accessed: Sep 8, 2022; .

40. Vaas L. Fitbit data leads to arrest of 90-year-old in stepdaughter's murder. https://nakedsecurity.sophos.com/2018/10/08/fitbit-data-leads-to-arrest-of-90-year-old-in-stepdaughters-murder/, note = Accessed: Sep 8, 2022; .

41. Newsroom SV. FitBit Murder Suspect Dies in Santa Clara County Jail. https://www.sanjoseinside.com/news/fitbit-murder-suspect-des-in-santa-clara-county-jail/, note = Accessed: Sep 8, 2022; .

42. Sharman J. Driver chased moped rider after wing mirror broken, ran him down then beat him as he lay dying. https://www.independent.co.uk/news/uk/crime/enfield-mustang-driver-hit-run-murder-sohban-khan-bradley-clifford-london-a8333201.html/, note = Accessed: Sep 8, 2022; .

43. LeMere B, Bollo J. A rapidly growing source of critical digital evidence, Evidence Technology Magazine. https://read.nxtbook.com/wordsmith/evidence_technology/winter_2018/vehicle_forensics_a_rapidly_g.html/, note = Accessed: Sep 8, 2022; .

44. Tanwar S. *Fog Data Analytics for IoT Applications: Next Generation Process Model with State of the Art Technologies* . 2020

45. Press TA. Man charged with arson after police read his pacemaker data. https://globalnews.ca/news/3245884/man-charged-with-arson-after-police-read-his-pacemaker-data/, note = Accessed: Sep 8, 2022; .

46. Pack L. Prosecutor: Man awaiting arson trial in Middletown pacemaker case dies, Dayton Daily News. https://www.daytondailynews.com/news/crime--law/prosecutor-man-awaiting-arson-trial-middletown-pacemaker-case-dies/PORi20NIKa8ONyVZis7RvN/, note = Accessed: Sep 8, 2022; .

47. Byun JY, Nasridinov A, Park YH. Internet of things for smart crime detection. *Contemporary Engineering Sciences* 2014; 7(15): 749–754.

48. Valle dJM, Souza G, Cacho N, et al. Using Traces from IoT Devices to Solve Criminal Cases. In: 2020 IEEE 6th World Forum on Internet of Things (WF-IoT). ; 2020: 1–6.