The Complexity of Internet of Things Forensics: A State-of-the-Art Review

Pantaleon Lutta
School of Computing and Digital Technologies
Staffordshire University
Stoke-on-Trent, UK
pantaleon.lutta@research.staffs.ac.uk

Mohamed Sedky
School of Computing and Digital Technologies
Staffordshire University
Stoke-on-Trent, UK
m.h.sedky@staffs.ac.uk

Mohamed Hassan
School of Computing and Digital Technologies
Staffordshire University
Stoke-on-Trent, UK
mohamed.hassan@staffs.ac.uk

Uchitha Jayawickrama
School of Business and Economics
Loughborough University
Loughborough, UK
u.jayawickrama@lboro.ac.uk

Benhur Bakhtiari Bastaki
School of Computing and Digital Technologies
Staffordshire University
Stoke-on-Trent, UK
b.b.bastaki@staffs.ac.uk

Abstract— **The rapid growth and usefulness of Internet of Things (IoT) has seen it being deployed in critical and strategic infrastructure sectors like healthcare, transport, agriculture, home automation, and smart industries among many others. The benefits of comfort and reliability of IoT technologies to human beings have brought with them security concerns. This is due to its large-scale connectivity and over reliance on the internet for communication making it susceptible to cyberattacks. Digital forensics experts face a daunting task of handling these cyberattacks because of the unique and complex challenges posed by IoT. Recently, researchers have been drawn to finding solutions to these challenges, however, this is still in its infancy. This paper carries out a Systematic Literature Review (SLR) of the current research advancements in IoT forensics. We define key IoT fundamentals, IoT applications, the need for IoT forensics, identify the key factors affecting IoT forensics, and review the practicality of the available IoT forensics frameworks, models, and methodologies. The SLR reveals research gaps indicating that most of the current research is more theoretical than practical. There is a need for more practical approaches to tackle the unique IoT forensics challenges. Finally, for future research directions from the SLR, we have highlighted and discussed the open challenges and requirements for IoT forensics.**

Keywords— Internet of Things, Digital Forensics, Cloud of Things, Cybercrime, Systematic Literature Review, IoT Challenges.

I. Introduction

The continued growth of IoT devices has enabled the sharing of information within people and between the devices themselves. The direct communication between these devices is facilitated over the internet by the Application Programming Interface (API) and is controlled by intelligent devices of the cloud servers that enhance smartness to low-computing resource incapacitated IoT devices[1].

There are indeed many beneficial aspects brought about by IoT applications more so in the areas of transportation (automotive), retail, health care, engineering, construction, smart cities and many others[2]. According to a report by Cisco [3] on the state of IoT, by the year 2030, it is expected that over 500 billion devices will be connected by the internet. The report also states that the IoT business is estimated to have a revenue turnover of around 14.4 trillion dollars by the year 2022. This revelation indeed shows that the human population has already been surpassed by the number of connected IoT devices.

IoT devices have limited computing capabilities in relation to processing and storage of data, due to this, [4] note that IoT environments make extensive use of the cloud computing services. The authors further depict that as result of the continued growth of customers for cloud-based services, it is evident that there is growing over dependency on cloud-storage media. This translates to the need for having digital forensics tools that are able to handle large volumes of data so as to extract data that could be of potential evidence. There is also a need for training forensic investigators on how to collect evidence from the cloud. As is always the case in most forensic processes, it can be a time-consuming exercise as forensic tools may take a lot of time to analyse huge amounts of data. This results in a slow forensic examination process thereby complicating and making it hard, more so in the collection of data from the cloud which could be stored in distributed locations.

Despite this positive outlook of the emergence of IoT technologies, it brings with it various security attacks and threats as noted by [5]. These threats could be in form of attacks from viruses, illegal surveillance, Denial of Service (DOS) attacks among other many threats and attacks. Digital forensics experts are often times called in to investigate these incidences.

It is unfortunate that in the design and development of IoT devices, not much attention is paid to the security leaving them exposed to susceptible threats. This gives room for hackers who exploit IoT devices' vulnerabilities and carry out illegal activities that cripple the cyberspace.

IoT forensic process brings with it unique and complex challenges. This is because digital investigators are required to create new investigative processes that are specific to IoT by drawing upon techniques and methods used in acquiring evidence from other established areas of digital forensics. The evidence in IoT devices is different from the traditional digital device (computers and mobile phones), this is because data from IoT devices can be in vendor specific formats that deviate from the normal electronic documents or file system formats.

It is evident as noted by [6], that the IoT systems' complexity together with the inadequate or even no unified standards hinder the process of digital forensics by preventing the acquisition of valuable digital evidence by Law Enforcement

Agencies (LEA) from IoT based forensic cases. The authors also concur that the available traditional methods, tools, and standards for digital forensics are unable to handle the highly heterogeneous and the IoT infrastructure that is distributed across the globe.

As highlighted by [4], even though research in digital forensics in cloud forensics is essential, much of the current research has focused more on the challenges encountered when carrying out digital forensic investigations in the cloud. There is minimal research that has proposed solutions that can be used to work around these challenges through practical models for digital forensics in the cloud. A lot of the available research focuses more on data storage, access control and the security of data in the cloud. The recent emergence of IoT which extensively uses the cloud computing platforms, it has become necessary to find solutions that are able to aid the forensic process.

As observed by [1], many surveys have been conducted in the digital forensics interdisciplinary domains such as mobile phones, smart cities, cloud computing, wireless networks and smart transport systems. However, these researches do not conclusively tackle the IoT challenges. The authors proceed and state that many studies have been conducted on IoT security rather than IoT forensics.

Even though many conceptual models and frameworks have been developed to try and solve the complex challenging characteristics of IoT forensics process, there still exist many unresolved challenges [7]. This is further highlighted by [8] who note that most research that relate to the digital forensic investigative process in IoT is more theoretical than practical. Generally, as also observed by [9], the forensic process of IoT is still in its early stages, there are few and limited researches that have been conducted. The conducted research, however, lack in-depth analysis and experimental results which could be as a result of unavailable testing data from IoT devices and/or limited IoT environments. On the other hand, the few researches with experimental tested models are specialised to specific scenarios which means that they cannot be used for general wholesome IoT forensic investigation processes.

Additionally, as noted by [10], that not much room for forensic analysis is provided for by the currently developed IoT solutions. The authors further claim that due to the limited computing resource capabilities for many IoT devices coupled with the unique cloud-based infrastructure makes it even difficult to store data in the devices for forensic purposes. Most popular IoT programming platforms like Samsung SmartThings, openHab and others do not provide any means to have access and indefinitely store data in the cloud.

II. INTERNET OF THINGS

1) Fundamentals of IoT

IoT being an emerging technology allows small devices (things) to perform tasks as smart objects. The interconnection between these devices (things) is facilitated by different network media types. The communication between the devices generally in making applicable decisions through the sensor data read.

2) IoT Applications

IoT technology can be applied among various application areas for example in home automation, wearable technology, smart environment, smart retail, smart industry, transportation, health, and Agricultural farming. This is best illustrated in the figure 1 below:

3) IoT Forensics

The word forensics can loosely be referred to as the application of science and technology in an investigation process for the purpose of establishing facts in a criminal or a civil litigation.

Digital forensics is a discipline that combines the basics of computer science and laws where the collected digital data (evidence) is analysed and presented as admissible in a court of law for prosecution purposes.

Forensic computing is a process that involves the identification, preservation, acquisition of data of potential evidence and analysis of the data to produce a report to be presented in a court of law in a way that follows the laid down procedures and acceptable laws in a particular jurisdiction.

IoT forensics can therefore be termed as a process of applying the process of digital forensics in a setup that contains IoT devices.

The authors [11] have defined IoT forensics by combining three digital forensics levels, namely: device, network, and cloud level forensics. The device level forensics involves collection of local memory data from IoT devices. The network level forensics is where network logs are extracted and analysed. Finally, the cloud level forensics involves analysing the data generated and stored by IoT devices to the cloud services. The cloud services serve a huge role in IoT operations. This is due to IoT devices having low storage and computational capacity thereby relying heavily on the cloud services which offer benefits like convenience, large capacity, scalability, and on-demand accessibility.

4) Why IoT Forensics?

Digital forensics investigation process has been vibrant recently due to the emergence of IoT technology which is now seen as a big threat to information security. The large volumes of data generated by IoT devices and in turn reshared between the devices contains a huge potential of evidential data due to the large number and variety of IoT devices that are spread within a wider application area.

As noted by [7], the digital evidence retrieved from an IoT setup can be useful because the evidence can be used by parties involved to support or contest any hypothesis claimed in the investigation process. This can be referenced to a New York Times report by [12] where a murder case was determined by data from a wearable device (fitbit). The complexity around the extraction of data from IoT environments is a major setback in the ability of producing evidence that is legally admissible in a court of law [6]. These complexities are attributed to the following reasons as brought out by [13].

- The huge uncertainty of the originality of data, the storage mechanisms, and the attributes associated with the data
- The struggle of to secure and maintain a chain of custody because of the highly volatile data

- The difficulty in applying the traditional digital forensics tools to extract data which could be stored on the cloud
- Legal complexities due to cross-border jurisdiction and service level agreements
- Varied and proprietary storage mechanisms of data which has very limited visibility due to IoT devices being resource constrained.

III. SYSTEMATIC LITERATURE REVIEW METHODOLOGY

To our knowledge, our review of the literature on IoT forensics revealed that there is limited previously published SLR in this domain.

This SLR adapts the search methodology guidelines proposed by [14].

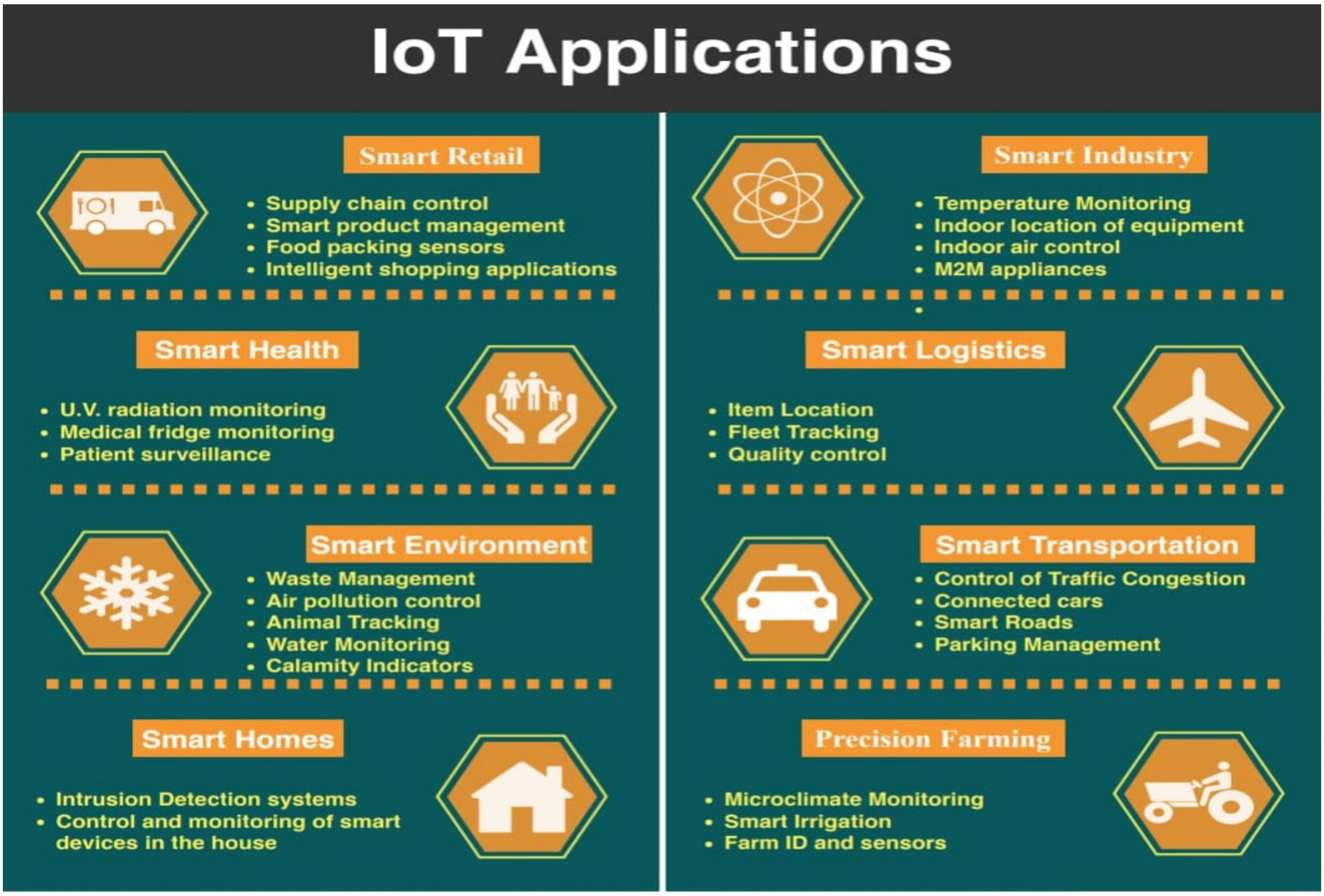

Figure 1 IoT Application

1) *SLR Aim*

To review the current state of research in relation to IoT forensics, expose the key challenging factors, explore the practicality of the reviewed literature, and discuss open issues and requirements for future research directions.

2) *Research Questions*

i) What are the key factors affecting IoT Forensics?
ii) What are the current IoT forensic methodologies, models, and frameworks?
iii) How practical and realistic are these methodologies, models, and frameworks?
iv) What are the open challenges and requirements for future research directions?

3) *Search Method*

The strategy used to find relevant literature are presented in the search protocol that answers the research questions.

4) *Database*

The online databases used in this review were; IEEE Xplore, Springer Link, ACM Digital Library, Wiley Online Library, Science Direct, and Google Scholar.

5) *Search String*

The usefulness of a search string is to capture the keywords in the research questions to find the desired results. To connect the keywords, the search employed Boolean operators (AND and OR). To attain exact words, the quotation marks were used, and the search string was:
("Digital forensic framework" OR "Digital forensic methodology" OR "Digital forensic model" OR "Digital forensic challenges") AND ("IoT" OR "Internet of Things" OR "Smart homes" OR "Cloud of things")

6) *Search Procedure and Selection*

The search string was executed on the online databases, from the results, keywords from the titles were read so that irrelevant papers were filtered out. For further refining of the results, the search applied inclusion and exclusion criteria to analyse the abstracts and full text reading.

The exclusion phase was done by excluding papers that are not peer reviewed, and papers of low quality and without any scientific basis.

The inclusion was based on online published papers from 2011 to 2018 and only studies that are in digital forensics field and IoT forensics in particular.

Further exclusion exercise to refine the results was based on non-English papers.

Figure 2 below illustrates a flowchart that summarises the search methodology employed.

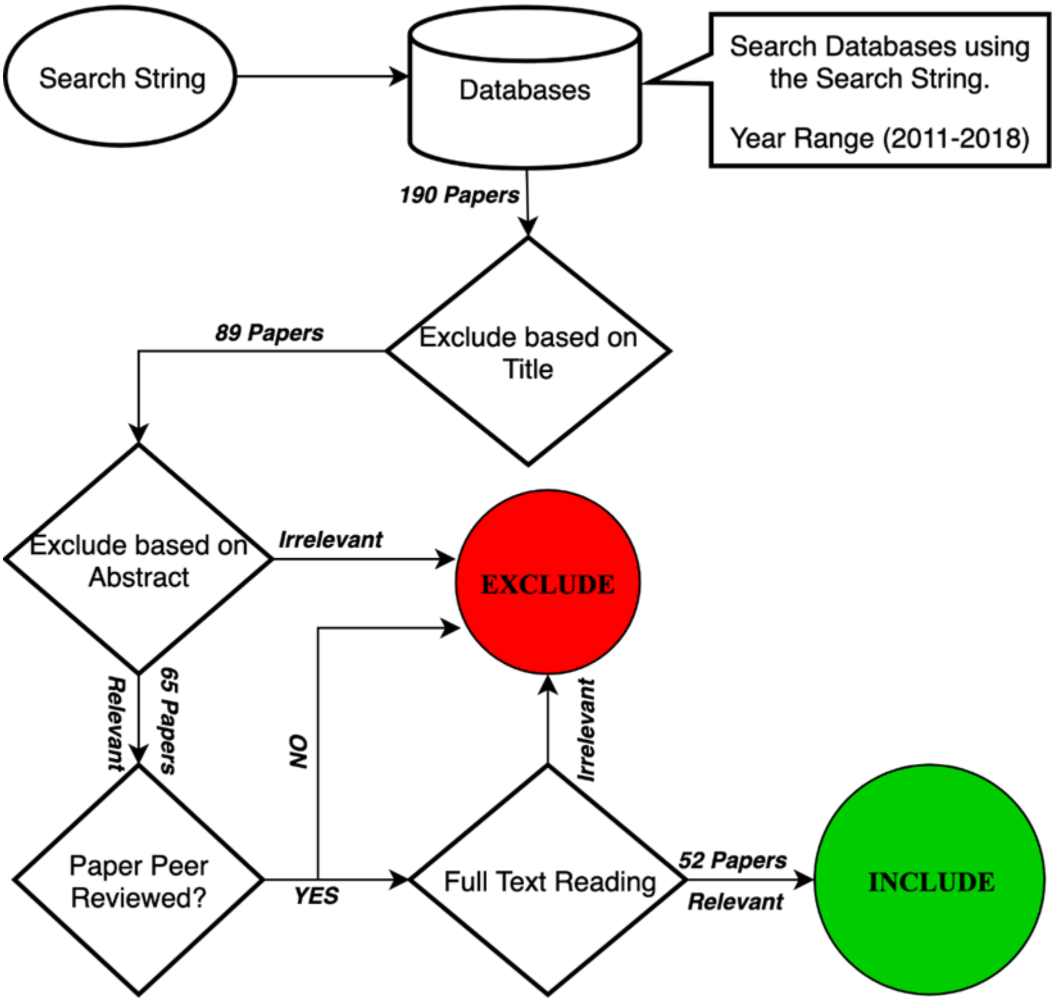

Figure 2 Search Method Flowchart

7) *Search Results*

Table 1 below shows the search results obtained from the five databases used. It was based on the exclusion and inclusion criteria adopted by this paper to arrive at the included papers.

Database	No. of Papers	Filter Based on Title	Filter Based on Abstract	Filter Based on Full Text Reading
Science Direct	11	5	3	2
IEEE	43	35	31	25
ACM	17	10	5	4
Wiley Online Library	25	6	3	3

Springer Link	23	12	11	10
Others	71	21	12	8

Table 1 Search Results

Figure 2 below shows the research papers distributed over time based on the review process of the scientific publishers like Science Direct, IEE, ACM, Wiley Online Library and Springer Link. In the classification, the SLR method uses the electronic databases according to Table 1 above.

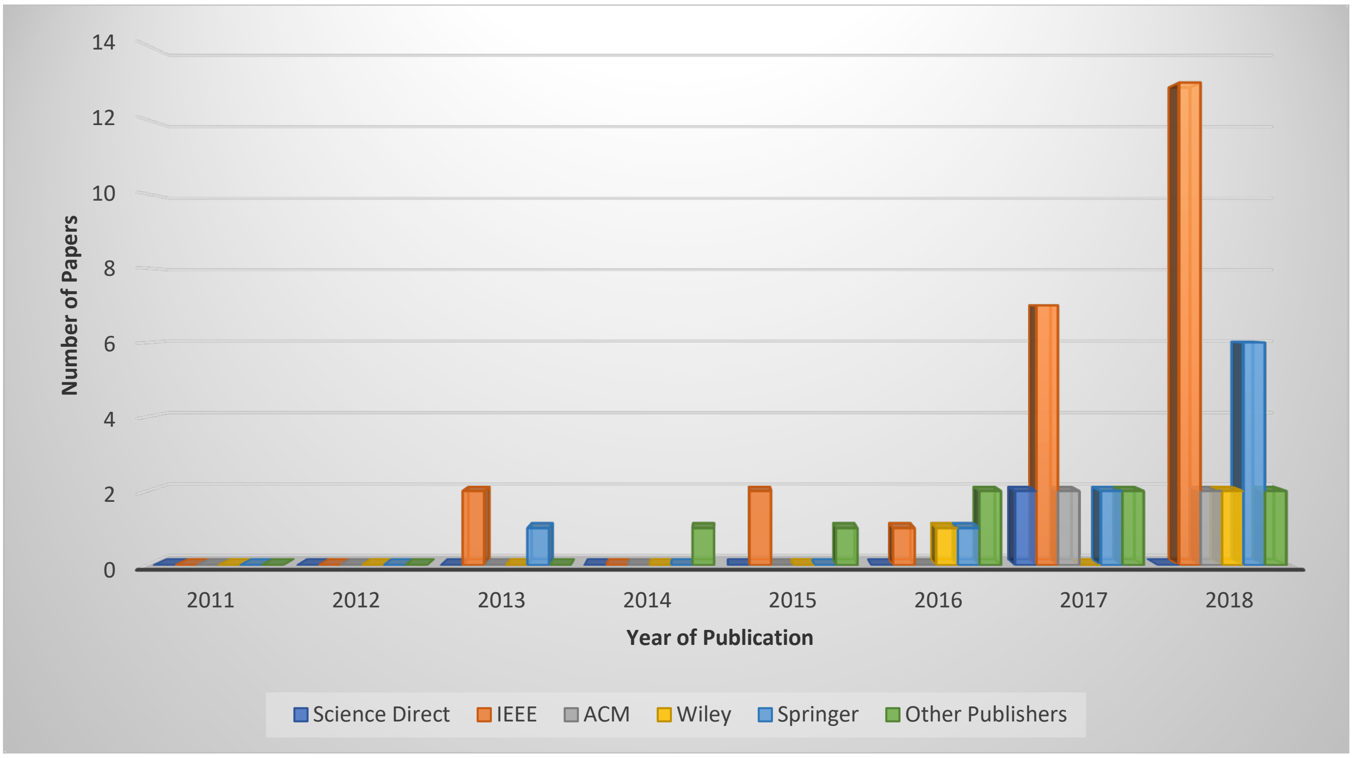

Figure 3 Distribution of Research Papers by Publisher

IV. FACTORS AFFECTING IoT FORENSICS

The complex and unique challenges brought about by IoT environments in relation to forensic investigative process have attracted recent advancements in the research. These efforts are however still in their early stages of development and majorly focusing on the theoretical process models based on hypothetical case studies [9].

Key IoT challenges that pose difficulties in digital forensics investigations are established by [13]. The authors identify fundamental areas that researchers should focus to provide solutions. The paper takes a view of the traditional digital forensics process (identification, preservation, analysis, and presentation) and relates it to how it can fit into IoT forensic, however, the authors did not perform any practical analysis for implementation.

Figure 4 below depicts the challenges:

1) Digital Evidence

The authors [1] lament that the key challenges exhibited by the huge data to the investigators are the varied data formats and the limited solutions for real-time log analysis. The short survival period and the limited visibility of the evidence can also be viewed as challenges to the investigation process more so in the circumstances where traditional digital forensics processes are applied in IoT forensics.

2) Big IoT Data

Due to the large data generated by IoT devices which are resource constrained and diversified across a huge spectrum. It is noted by [1] that this large data generated presents digital forensics expert the difficulty of collecting and extracting evidential data in a smooth manner.

A research by [15] summarises the review on digital forensics trends used for Big Data and the challenges encountered in the acquisition of evidence. A Smart City project is used as a case study where IoT services collect Big Data and store it in the cloud. The authors note that one of the major challenges of the forensic process is as a result of the distributed nature of the cloud environment making it very difficult for the data acquisition techniques to retrieve evidence. In the case study, an example is given of a driverless car (public transport vehicle) which sends huge amounts of data to the cloud. This data is in turn used to control the operations of the car and provide local information by suggesting the best services to the customers. A scenario is created where this data is hacked into and the car is crashed. It is depicted that it would be hard for a digital forensic investigator to again access to the data. The paper does not provide any viable solution to the challenges it highlights; however, it provides a summary of the challenges that have been solved and not solved under what cloud service which could be beneficial to the research community.

A research by [16] discusses IoT forensics and brings out its uniqueness of IoT forensics to traditional forensics by highlighting the challenges encountered. In their experiments, the authors used a smartwatch as a case study and described how to acquire forensic data from an apple smartwatch. The three levels of IoT forensics (device, network, and cloud) have been emphasised. The paper describes the main challenges of IoT as; location of data, limitation of digital media due to lifespan, weak requirements signing up for cloud services, lack of security in IoT devices, device type identification, and the proprietary data formats. The limitation of the currently available forensic tools to handle IoT forensics has also been discussed, this is more so stressed by the fact that most of the IoT data is found in the cloud and not many forensic tools can collect data in the could be due to the data volatility. In their conclusion, the authors concur that there is need to develop an efficient generic model to handle IoT forensics.

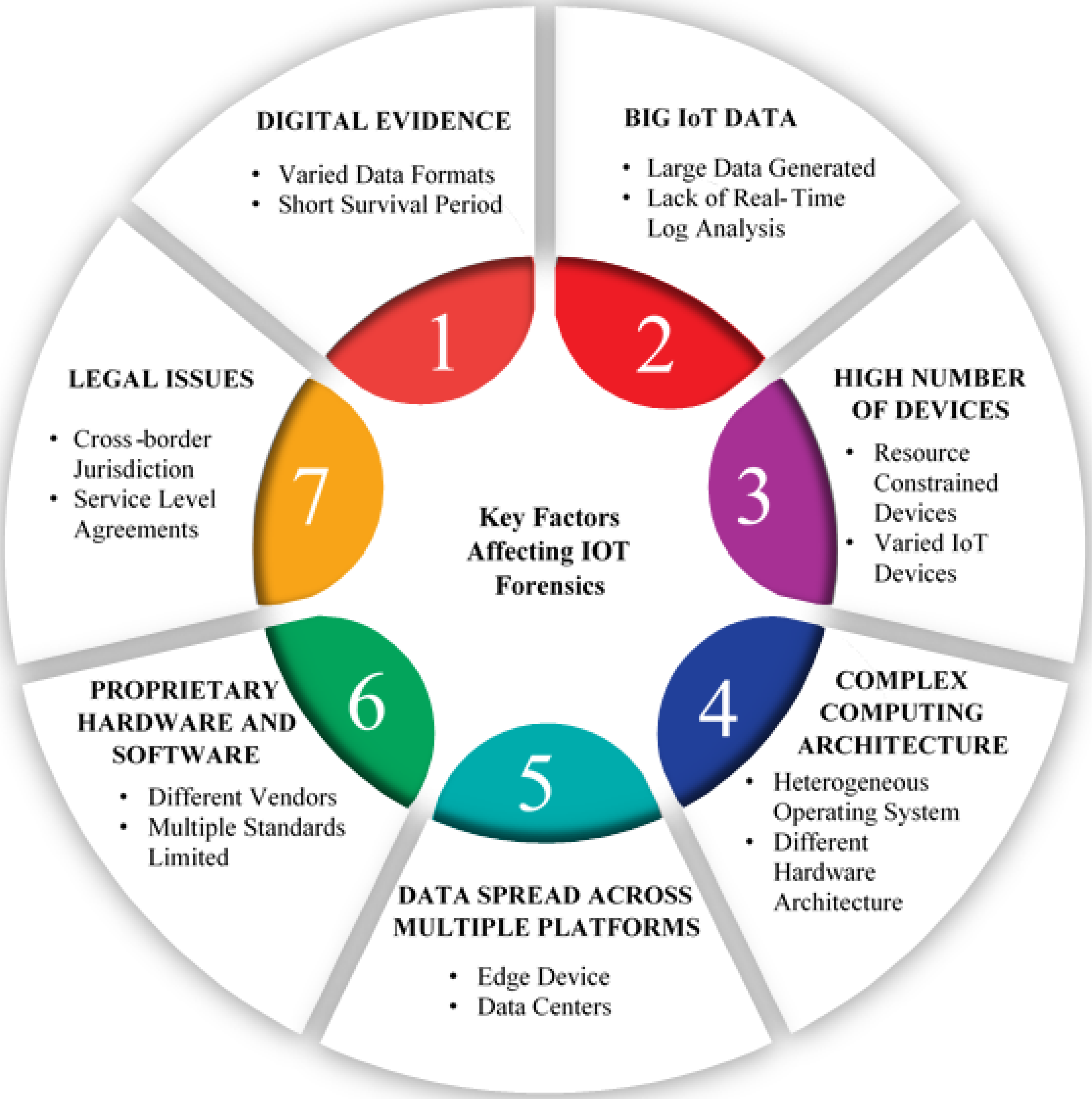
DIGITAL EVIDENCE
• Varied Data Formats
• Short Survival Period
BIG IoT DATA
• Large Data Generated
• Lack of Real-Time Log Analysis
HIGH NUMBER OF DEVICES
• Resource Constrained Devices
• Varied IoT Devices
COMPLEX COMPUTING ARCHITECTURE
• Heterogeneous Operating System
• Different Hardware Architecture
DATA SPREAD ACROSS MULTIPLE PLATFORMS
• Edge Device
• Data Centers
PROPRIETARY HARDWARE AND SOFTWARE
• Different Vendors
• Multiple Standards Limited
LEGAL ISSUES
• Cross-border Jurisdiction
• Service Level Agreements
1
2
3
4
5
6
7
Key Factors Affecting IOT Forensics

Figure 4 Factors affecting IoT Forensics

The challenges encountered IoT's big data ecosystem and recent IoT applications are highlighted by [17]. They observed that there is need for tools and libraries for better management of IoT-big data.

3) High Number of Devices Spread across the Globe

IoT forensics challenges are looked at by [18] with a view of Internet of Anything (IoA) era. The IoA is depicted by the author as an explosion of connected devices due to anything and everything online being connected. The author state that the main forensic challenge of IoT/IoA is the procedure for the acquisition of data in those connected devices.

The laws surrounding accessing data in the cloud are looked at by [19]. Given that the cloud stores a huge amount of data transmitted between IoT devices, the author states that one of the major challenges that digital investigators face is the collection of data in the cloud setup. Cross-border cooperation for mutual legal assistance should be encouraged to enable acquisition of data from different territories. The same challenges were also raised by [20].

4) Complex Computing Architecture

As highlighted by [11], IoT devices have limited computing capabilities and rely heavily on cloud services for their functionalities. It therefore follows that data will be collected from the cloud infrastructures and analysed leading to a form of cloud forensics investigation.

The complex challenges in cloud forensics are highlighted by the authors [21] who acknowledge that evidence can vary significantly when collected via Virtual Machines (VMs) from multiple cloud deployment models; the authors recommended a service-specific solution. An example is given where if evidence was to be collected from an Infrastructure as a Service (IaaS) environment, it is recommended that collection is done by use of snapshot analysis or creation of forensic images through cloning. The setback with this solution is that it is not feasible for cloud service providers to clone all their cloud servers as this will require a lot of storage space.

A survey authored by [22] seeks to analyse the state of cyber-crime in IoT environments. The authors discussed issues relating to how the traditional digital forensics methodologies could be integrated into IoT cases. The authors clearly indicated the types of crimes in IoT and where potential evidential data could reside in cloud environments and how to extract. However, the authors failed to carry out any practical example of how to implement their recommendations leaving the paper more theoretical than practical.

5) Data Spread across Multiple Platforms

Three layers (cloud/server, network and endpoints) are outlined by [23] where potential evidence can be located. The author attempted to identify issues and challenges encountered during acquisition of evidence from IoT environments in a crime scene. Even though one of the author’s aim was to help investigators in acquiring data from IoT crime scenes, there is no practical example to illustrate the same.

The challenges of forensic analysis encountered at the physical infrastructure on whose basis lies the operating systems of Industrial IoT (IIoT) are highlighted by [24]. A review of the available tools that can handle a forensic process of Supervisory Control and Data Acquisition (SCADA) is done resulting into a SCADA incident response model.

6) Proprietary Hardware and Software

According to [25], the data from IoT devices is heterogeneous unlike the data from traditional data devices. The author further note that IoT data may stream at rates that are unpredictable. Additionally, the security and privacy measures employed in many IoT devices do not address issues like ownership, management, and regulations.

The forensic challenges faced by vehicular fog computing are highlighted by [26] who pointed out the difficulty in physically checking every fog node deployed in the system. The authors, however, provided countermeasures like evidence based digital forensic and traffic-based evidence approach.

7) The Legal Challenges

The prevalence of IoT enhancement through approaches that leverage big data techniques for the purposes of improving the assurance of information are surveyed by [27]. The author notes that it is expected that IoT will stress the organisational frameworks in relation to the current technical and legal spectrum. This will however be significant more so in forensics and safety audits. The nature of work for information security experts, forensic investigators and system auditors has been hugely changed by the prevalence of Big Data. It is more complicated by the emergence of IoT devices that add huge volumes and various forms of work to be performed by these experts.

A survey conducted by [28] reviewed cloud computing and internet of things (both combined as “cloud of things”) in relation to key legal issues emanating from European Union (EU). The wider perspective on legal and regulatory aspects of cloud of things, major challenges, and complexities in the past, present, and future are highlighted.

The following aspects are covered at length in the survey:

- Cloud of things concepts and challenges are explained in relation to the definition of “things”, what they do, how they communicate and the role of the clouds and their security challenges thereof.
- Legal relationships and liabilities involved in cloud of things; the establishment of different parties in cloud of things and their relevant roles, the contractual obligations, the ownership of the data and software intricated in cloud of things, and the potential sources of liability and the role played by the insurance.
- Handling of personal data in cloud of things; issues related to personal data in the cloud of things under the EU data protection laws and General Data Protection Regulations (GDPR), expounding on what data is regulated, to whom the responsibility falls, the

applicable laws, what rights do users have over their data, the location, and transfers of the data.

- The governance of cloud of things; tackles the key issues relating to identity, authenticity and trust, consumer protection, standards and the demonstration of how legal obligations can be complied.

The paper outlined the various fundamental legal considerations as presently portrayed in the cloud of things. Although nothing much has been covered in relation to cloud and IoT forensics, this research is deemed resourceful in the application of laws in the process of IoT forensics. However, the laws are only limited to EU regions.

There is no physical access of the storage facilities and that digital forensics investigators rely heavily on the Cloud Service Providers (CSP) for cooperation on the retrieval of evidence, this was highlighted by [15]. The cross-border technicalities that make it hard to establish a chain of custody as required by law have been highlighted as a challenge to IoT forensics.

A paper by [29] analysed IoT and smart cities in relation to the legal challenges encountered in digital forensics, privacy and security and noted that competence of digital forensics experts in matters law was a major hinderance. The authors did a comparative review of legal regimes in China, Korea, Hungary, European Union, and the United States of America, analysing how digital forensics and investigations are carried out. The GDPR of the EU has been identified as well-defined to aid the process. The authors state that the US case decisions can be a basis for analysing current legal problems paving way for future regulations. They conclude by stating that the legislation needs to be clear on issues relating to the balance between public security and individual privacy freedoms.

It is noted by [23] that unlike in traditional digital forensics where the process is well defined by the National Institute of Standards and Technology (NIST), no specific guidelines are provided for in an IoT crime scenario.

The solutions suggested by [21] are based on different use cases like the verification of Service Level Agreement (SLA) and enforcement of compliance aspects.

V. THE CURRENT STUDIES IN IoT FORENSICS

The current digital forensics approaches in the internet of things have been surveyed by [30]. They have highlighted the gaps and limitation of the papers they sampled and indicated that there is indeed need for an improved proactive model under which IoT crime scenarios can be handled.

In their conclusion, the authors claim that none of the frameworks and models proposed from the sampled papers can be used to extract data in a timely and reliable way.

There have been a handful of proposed IoT forensic processes that have included methodologies, models and frameworks which have contributed to the advancement of research in this area.

These processes are discussed below:

1) Next Big Thing

The Next Big Thing process model was developed by [31], in this research, the authors propose a process model based on the challenges faced in the identification phase of the IoT forensic process. It was designed to help in the determination of potential sources of evidence. The triage is presented in a 1-2-3 zone approach whereby zone 1 consists of the identification of the person involved in the crime and potential evidence to be identified. Zone 2 covers all the possible devices within the network (routers, firewalls, switches, intrusion detection systems (IDS) and gateways). All the devices and services (web, database, and cloud servers) outside the network are identified in Zone 3. This process model considers the fact that any potential evidence stored in the devices could easily become unavailable due to theft, tampering, or destructed. With this realisation, other elements within the IoT environment related to the evidence must be recognised by the investigator because they may contain valuable artifacts to aid the investigation process.

This process can be beneficial to the IoT forensics process more so in the identification phase. The challenge with this process model, however, is the development and testing. This is because it cannot be assumed that the investigator will have direct access to all the devices or even the cloud servers where the evidence could be stored. The resource limited IoT devices and the volatility of the cloud needs to be considered. The process does not also have clear laid down directions for investigation to follow while conducting the analysis.

The Next Big Thing was later integrated by [32] through the top down forensic approach methodology which was designed to provide a novel approach that enables IoT forensics investigators through defined Standard Operating Procedures (SOPs). It is an integrated model of the 1-2-3 zone model. The top-down forensics approach methodology tries to solve the challenge to do with the preservation of volatile data. Previous approaches in digital forensic investigations were vigorously conducted by this study. The study proposed approaches that can be helpful to the investigators of IoT environments. The setback is that it may not be feasible to implement its automation in a real practical environment as the authors have also not tested it practically.

Last on Scene (LoS) algorithm was proposed by [9] as a model based on the Next Big Thing process model. The LoS algorithm works by identifying the location of evidence in such a way the first device to be investigated is one that was seen last on communication chain. The authors of the LoS algorithm model claim that the model saves time and resources for digital investigators because only data of interest is sought, and therefore if found in zone 1 the process terminates, and a report is compiled. The investigators do not have to go through all the zones looking for potential evidence.

As implied by the authors themselves, the LoS Algorithm is a theoretical framework meaning that its practical implementation or application has not been performed. The legal implication aspect has also not been factored into this framework; this means that it may not be admissible in a court of law.

2) Forensic-Aware IoT (FAIoT) model

Designed by [11], this model encapsulates the IoT digital forensic processes and techniques. The authors define the term IoT forensics process in three levels of digital forensics: device, network, and cloud level forensics.

The model employs a secure trusted central repository that aims to deal with the problem of IoT domain not being standardised. A chain of custody being a key part of a digital forensic investigative process, this model focuses on ensuring that a chain of custody is maintained. Unfortunately, there is no practical implementation of this model.

3) Digital Forensic Investigation Framework for IoT (DFIF-IoT)

Proposed by [6], this process model is based on a generic approach that analyses digital forensics data in the IoT setup through process concurrency. The model is presented to capture data at all the three levels of the IoT forensics.

Through the process concurrency, the model aims to establish IoT forensics readiness and increase the rate at which the digital evidence extracted is admissible in a court of law. From the readiness point of view, this model will require a momentous consideration to proactive scenario-driven activities to ensure that the potential evidence is captured with the IoT setup and that implementation for extraction and preservation of the evidence is done in a procedure that is well-defined and documented. It is through this that the evidence will be forensically sound.

The drawback with this model, however, is that it is purely based on theoretical approach in the collection of the forensic data. There is no physical experimental in its implementation and evaluation thereby casting doubts on its practicality.

As an extension of DFIF-IoT, [33] proposed an Integrated Digital Forensic Investigation Framework (IDFIF-IoT) which claimed that DFIF-IoT was generic with processes that relied on ISO/IEC 27043 international standards while IDFIF-IoT includes organisational policy making it more policy oriented.

This framework is still more theoretical than practical and as also pointed out by the authors themselves, the framework needs more development so as to identify more critical aspects of forensics.

4) IoT mobility forensics model

The authors, [34] explored the mobility forensics in its context to IoT. The process of data acquisition and the classification methods for smart home devices are discussed in detail. An analysis of an attack scenario of the collected data is also discussed and a model is proposed that handles such scenarios. The proposed model seeks to address; what happened, when it happened, how it happened, who and/or what did it, why it happened and what data was collected?

This paper contains valuable information that can be used as a framework for controlled IoT forensic investigations. However, it is limited to only one device being tested. The model proposed was not implemented, deployed and neither was it tested. The authors also assumed the full availability of data, this is usually not the case for forensic investigations.

IoT mobility forensics model is used by [35] to describe a process of data retrieval from smart devices and how this data can be classified and analysed. An analysis was performed based on a scenario of attacking the collected data and proposing a forensic model that fits such scenarios. The authors claim to collect data using Wireshark; however, they do not reveal from where this data is preserved as this is very crucial in a criminal investigation. They do not also tell if this data is live data, and if yes, how can it be a criminal case when all is planned and acted? If no, where was this data stored? Internally or in the cloud?

In [36] experiments, mobility forensics is used whereby cookies are collected from kid trackers to locate a missing child. The forensic model proposed tries to establish what happened, why it happened, when it happened, how it happened, how data was collected, and what data is needed from the trackers. However, as also noted by the author, none of the processes proposed in the model have been tested or tried.

5) Cloud-Centric framework for isolating Big Data as Forensic Evidence from IoT Infrastructures (CFIBD-IoT)

The CFIBD-IoT framework proposed in this study consists of three layers. It recommended a standardised technique of how to acquire and isolate evidence.

Authored by [37], the research investigated how the spread of IoT has led to the complexity of the investigation process. A case study of BitTorrent is used as a focus point where cyber criminals have explored the avenues opened up by IoT through information theft and side channel attacks facilitating crime-as-a-service.

The anonymisation techniques have been used to hide the privacy of the users thereby allowing private communication, this has made it possible for cyber criminals to exploit the feature and attack IoT setups.

The challenge is that where are law enforcement agencies may get access to the client machine, they may not have access to evidence that may be stored in the cloud.

6) Privacy-aware IoT-Forensic (PRoFIT) Model

The PRoFIT model proposed by [38] incorporates privacy in its investigation process by making use of the requirements of ISO/IEC 29100:2011. Assurance for privacy encourages IoT devices to participate in digital forensics investigations in a voluntary basis. The model emphasises on the importance of collaboration between devices that are nearby to aid in the collection of the evidence and determine the context within which the crime falls. This makes it ideal to fit into a concept of a digital witness. The evaluation of the proposed model was conducted in a coffee shop which was IoT enabled with an actual malware propagation.

Like many other models proposed, the PRoFIT model lacks the practical part and therefore remains a theoretical model.

7) Fog-Based Digital Forensics Investigation Framework (FoBI)

A research by [4], FoBI utilises the fog computing model by which intelligence is pushed by a gateway to the network edge. An example is given whereby a last known location of a device can be traced and any malfunction can also be identified using the log files.

When a suspicious activity is found during the FOBI investigation analysis, the nodes or other IoT devices are notified of the potential threat so that the propagation of the threat to other IoT devices it minimised or eliminated.

The FoBI framework, though workable, is not suitable for a general IoT forensic investigation. It can well be implemented in a home or a controlled environment and its main purpose would be to track user activities and notify of any suspicious activities. The fact that a FoBI management software has to be installed on a node or a gateway may raise questions related to surveillance and may fail the test of judicial process in a court of law.

8) IoTDots

A research by [10], IoTDots is a novel digital forensics framework for smart environments. It comprises of IoTDots-Modifier (ITM) and IoTDots-Analyzer (ITA) as the main components.

Through the ITM, applications on the smart device are able to be analysed by way of looking for relevant information that can be of forensic value. The applications on the smart device are then modified by insertion of particular logs which in turn send the forensically relevant data to the IoTDots Logs Database (ITLD) at runtime.

During the forensic investigation process, data processing and machine learning techniques are applied through the ITA on the ITLD data. This process involves the learning of the state of the IoT environment and the behaviour of the users in the time of interest of the forensic process. Violations are then identified by the events and actions against the security policies put in place.

This framework is one of its kind in IoT forensics as it has practical and experimental evidence. However, it is specific to a controlled group of IoT device users and may not be viable for random devices as IoT environments are flooded with many different devices. This is because, as rightly indicated by the authors, some IOT devices are resource constrained and may not have smart applications installed on them, this means that this framework cannot work on such devices.

Another drawback on this framework is that one of the components (IoTDots-Modifier) goes against the forensic principle of modification of the evidence and therefore may not pass the test of a court of law. The authors do not specify if they have the full consent of the users as per the European General Data Protection Regulations when installing these components on the devices.

Moreover, this framework appears to be a security framework rather than a forensic one because, critically studying it implies that it is a tracking system.

9) Digital Forensics Readiness for the Internet of Things (DFR-IoT)

A research by [39], the authors proposed an architecture that is able to forensically incorporate Digital Forensics Readiness (DFR) within the IoT environments by planning and preparing for any intrusion to the IoT setup. The authors stated that before their paper, there was no known model or framework that could incorporate DFR for the purpose of incident preparedness in IoT setups.

The framework has three distinct entities which are: Proactive Process (detects pre-incidents), IoT Communication Mechanism (provides smart communication strategies on the intelligent network for machine-to-machine devices) and Reactive Process (handles digital investigations in post-event response process).

Although this framework has a practical and experimental results, it does not show how the general digital forensics processes of preparation, identification, acquisition, preservation, analysis, and reporting. This is exhibited by its lack to show the chain of custody and the acquisition of potential data at all levels of IoT forensics (device, network and cloud levels). A practical demonstration of a report or a process that is admissible in a court of law needs to be specifically outlined and presented. The framework is based majorly on how an IoT environment can best prepare for a potential security incident.

10) A Forensic Investigation Framework for IoT (FIF-IoT) and Probe-IoT

FIF-IoT as described by [40] is a framework uses public digital ledger to forensically investigate IoT-based systems. The framework operates by storing in a Bitcoin-like public digital ledger all the interactions that the device makes with other devices, users, or cloud. The stored data is used as evidence. The setting of the framework allows evidence acquisition and also enables the verification of evidence during the investigation process.

This framework though well thought and explained; the experiments subjected on it cannot warrant its use for a forensic process that can stand the test of a court of law. The authors claim that there is integrity preserved yet they do not show how this is achieved in their experiments.

An IoT forensics framework proposed by [41] called Probe-IoT uses public digital ledger in searching for evidential facts in incidents in systems that are IoT based. Through the framework, interactions between IoT entities like IoT devices, IoT users and the cloud, are collected as evidence and stored securely in a Bitcoin like technology. The authors claim that Probe-IoT framework guarantees confidentiality, integrity, non-repudiation, and anonymity for the stored evidence data. This is because it is stored in public ledger. The framework also provides a mechanism in which during an investigation of a malicious incident, the integrity of the stored evidence is verified by authentication for any retrieval.

This research provides a tight security in accessing the evidence collected and can be extended to any evidence that is not necessarily IoT based. It would have been better if a real-life simulation of collection of data in a typical IoT forensic investigation was performed so as to show how this data is acquired. After the acquisition, the authors should have demonstrated how it is securely preserved using the framework and how its access by different parties as outlined in the paper is implemented.

11) Forensic Evidence Acquisition and Analysis System (FEAAS)

In this paper, the forensic artifacts retrieved from Nest's IoT devices (thermostat, indoor and outdoor cameras) are analysed by the authors, [42]. These devices were controlled by an iPhone. The source of the data from for the logical backup of the iPhone. Google Home Mini was also integrated by the authors as another method to control the Nest devices being studied. It is claimed by the authors that their work produced a first usable forensic tool named FEAAS from open-source research. The tool, as the authors state, consolidates evidentiary data into a readable report depicting user activities and what might have triggered the activities thereof.

From the experiments and the analysis done by the authors, it is evident that they had possession of all the devices and access to all the databases storage sites. The authors have simulated how smart home can be controlled and also given details of when, what, and how the events take place. All this information could be very valuable in a case as the investigators can get access to the relevant information. However, this is usually not the case in many digital forensic cases because in most cases, the investigators have no access to the control phone which in this case, the authors have retrieved the logical data from. The tool created could also be restricted to the mentioned devices alone.

12) IoT Device Forensics and Data Reduction

This research seeks to use data reduction which entails selectively imaging data. The acquisition process is automated and huge amount of data is quickly analysed in time. The authors, [43], state that the paper outlines a process of analysing huge volumes of data for forensic purposes. This data includes that from dissimilar devices.

It is noted by the authors that as many devices interconnect through the internet and upload huge amount of data to cloud platforms distributed around the globe, it is important to identify relevant potential data of evidence for forensic purposes. Securing of the crime scene is also problematic because the wireless crime scene may leak data as the investigators process physical devices.

The authors further note that the analysis of dissimilar devices is a challenge as many of these devices that flood the market do not adhere to forensic readiness principles. The data from these devices could as well be proprietary and the manufacturers are in most cases hesitant to give out details about the data structures used for fear of leaking their secret to their competitors. The reverse engineering that may be performed on this kind of devices may not pass the test of a court of law as the authors state.

Although the research was aimed at performing analysis in a faster way, the time taken for acquiring data in these experiments is still too much, there is need to look for mechanisms to ease the process of acquisition. However, there are useful forensic tools that the authors have proposed and used in their research that are very essential in the digital forensics' realm. The research cannot be fully relied on as the authors state that they had limited access to the data and could not therefore view or query the data to reveal the number of dissimilar devices contained in the data.

13) Other IoT Forensic Processes

The authors, [44] proposed two approaches for conducting IoT investigations based on low security mechanism and constraints encountered in IoT setups. The real time approach for IoT forensics proposed in this paper appears to be too general. The authors have implemented what is perceived to be done in traditional digital forensics into IoT forensics. This mode of approach will only work if the investigator has a full access to the device, the network and where the data is being transmitted to and/or from (maybe the cloud). It could be a measure for IoT forensics readiness in a controlled environment. No practical work has been performed by the authors to illustrate their proposals.

A summary is provided by [45] of methods to collect and analyse data to improve digital forensic process in IoT environments. Amazon Echo and Z-Wave devices as part of smart IoT devices together with a router were analysed to reveal important forensic evidence that can be extracted. This paper however lacks the practical solutions that can be applied in scenarios of the general IoT forensics as it focusses more on Amazon Echo, Z-Ware, and a home router.

A three-layered architecture is proposed by [46] which keeps track of the three level of the IoT forensics (device, network and cloud) and showcases where potential evidence can be found within those layers. The authors have outlined different types of open-source tools that can be used in every level but fail to give experiments on how this can be done. This research remains a theoretical work like many others.

A research by [47] focussed on the collection of data from IoT devices. The authors discussed the mode of data identification and the methodology of data classification from IoT devices to find the best available evidence. Tools and techniques to for identification and location of IoT devices are also proposed. The authors also claimed to develop a concept of "digital footprint" in the crime scene based on frequencies and interactions mapping between devices. The classification methodology used in this paper is too general and may be limiting to other IoT scenarios. The issues to do with synchronisation of data and the aspects that address the legal issues also need to be discussed further as the authors noted.

A framework is proposed by [48] for forensic investigation in IoT environments (smart homes). The authors simulated the three case studies to illustrate all the three levels of IoT forensics (device, network, and cloud). They claimed that their research fills the gap on how to acquire any type of data that may be potential evidence in a smart home setup. This framework looks to be very helpful to the digital forensic investigators, however, as these case studies are only simulations, it may be reasonable if the framework is applied in a real-life situation.

A forensic investigative framework is presented by [49] to be used in Industrial IoT applications. Their framework is based on the fact with which they allude that most forensics investigations happen at the higher layer digital domain meaning that the lowest layer domain remains hugely unexploited. They have therefore performed forensic investigations on the lowest physical layer of the network and illustrated what evidential data can be found within that lower physical level.

A framework called Trust-IoV is proposed by [50] whereby evidence that is trustworthy from internet of vehicles systems is collected and stored. From the experiment results of the framework, it is shown that in scenarios where there are strong adversaries, the framework can work with very minimal strains.

A proposal by [51] on a permission blockchain based mechanism for IoT forensics which enhances integrity, authenticity, non-repudiation in the process of collecting and preserving evidence.

The system provided [52] was aimed at providing security and forensics capabilities for smart homes. The strategies involved in this system can be helpful in an investigation more so for first responders as it has forensic readiness capabilities.

A framework is provided by [53] for acquiring data saved stored on the cloud by IoT devices. The setback in this framework is that the authors have not exhaustively provided the information relating to how they have developed their forensic tool and the tool only seems to work with android phones.

The acquisition of data, as shown by the authors [54], can be done both from the devices and the cloud. The author's Forensic State Acquisition from Internet of Things (FSAIoT) framework was however not possible to retrieve deleted or historical data from IoT devices. More experiments should also be done to reveal the extent to which varied IoT devices can be able to work with this framework.

A concept is proposed by [47] where traces of IoT devices can be tracked down and identified. A central bridge device is used to connect to other devices in the surroundings. The identified devices are ranked based on their importance of interest. The main setback with this concept is that the world is flooded with varied devices which may not be identified. [55] proposed an application specific IoT forensics investigative model where data is acquired, examined, and analysed resulting into a generated report.

The authors [56] proposed a national repository knowledge base for digital forensics experts. The knowledge base, with the necessary security control measures, could be expanded to allow for inclusion of methods that are suitable to aid in data reduction in a digital forensic process.

An investigation is done by [57]on how Machine Learning techniques can be used to develop a mechanism for network forensics to track suspicious activities of botnets based on network flow identifiers. This piece of work can be used to enhance IoT forensics especially in cases of compromised IoT devices through botnets, however, as it is an intrusion detection mechanism, it remains to be a forensics readiness process.

A forensic framework is proposed by [58] for big data in IoT environments for precision and sensitivity. The framework employs a Machine Learning (ML) approach using the Google's MapReduce as the basis for understanding traffic, extracting, and analysing the data. Open-source tools that support parallel processing and scalability have also been used in the framework. Comparatively analysed against other ML models, the framework exhibited a performance metrics of 99% sensitivity.

VI. Summary of the Research

The table below gives a summary of the discussed frameworks, models, and methodologies above. The categorisation is based on the limitations and gaps in relation to the practical view of the proposed research as applied in the IoT forensic process. The main features of these frameworks have been identified.

Authors	Main Features	Practical View of the Forensic Process	Limitations and Gaps
[21]	Service Specific solution for cloud forensics SLAs verification and compliance issues	Snapshot analysis or cloning in the Infrastructure as a Service cloud environment Evidence Identification and Acquisition	Not feasible for all data to be cloned by the cloud service providers
[31], [9], [41], and [54]	1-2-3 Zones of IoT Forensics Systematic and structured approach to minimise the complexity of IoT investigation processes Identification of more evidence sources in the absence of the primary source of evidence Last-on-Scene (LoS) algorithm Use of public digital ledgers to find evidence in IoT based systems FSAIoT	Mapping the investigation process and helping to identify key areas of focus. Devices of interest identified in the focus areas established Evidence Identification Guidance on the investigative process based on established zones	The identification of evidence is only partial Difficulty in the development and testing No clear instructions/directions on how to carry out the analysis and the whole investigative process
[6], [13], [22], [27]. [32], [11], [34], [36], [47], and [52]	Review of the current tools for forensic readiness in IoT Preserving of volatile data/evidence Evidence acquisition and preservation Maintaining chain of custody The proactive (readiness) and reactive (investigation) IoT forensic process Identification and acquisition of evidence	Theoretical	Practical aspect to augment the implementation, deployment, analysis and evaluation Too generic approaches may not be suitable for IoT forensics
[16], [37], [38], [42], [46], and [55]	Incorporates privacy in the forensic process using the requirements of ISO/IEC 29100:2011 Collaboration of nearby devices	Identification, acquisition, and analysis of data	More vigorous experiments to explore how the current tools can be used to fit into the proposed frameworks and solutions
[4], [10], [33], and [39]	Builds intelligence at the edge of the of the network through a gateway IoTDots-Modifier (ITM) and IoTDots-Analyzer (ITA)	Forensic readiness Incident preparedness	May fail the test of the judicial process due to installation of a management software which may be viewed as surveillance in a public setup. No clear instructions/directions on how to carry out the analysis and the whole investigative process
[40] and [51]	Uses Blockchain like mechanism for evidence preservation Provides privacy	Evidence preservation Chain of Custody	Vigorous experiments required for the purposes of admissibility in a court of law
[56]	Selective data imaging, automated acquisition and quick analysis	Identification and acquisition of data	Need for finding ways to reduce the time taken for acquisition of data

[48]	To identify and acquire any kind of evidential data in a Smart Home environment	Provides guidance for quick reference for investigation processes involving smart home environments All three levels of IoT forensics are covered	Application of the simulations used in this research should be carried out in a real-life scenario

Table 2 Summary Table

VII. DISCUSSIONS AND ANALYSIS OF THE RESEARCH

Open Challenges and Requirements

Most of the research surveyed by this SLR have proposed models and frameworks that have majorly focussed on conceptual levels that are more theoretical. Further investigation and research are required to tackle among others the following key issues as also emphasised by [7] and [1]:

1) Development of process models, methodologies and tools that are practical

Although sound principles have been applied in the proposed models and frameworks to tackle the complex challenges of IoT forensics, there still exists a need to conduct robust experiments that can be validated scientifically. Any new methodologies, techniques and tools developed must undergo a scientific validation.

2) Smart analysis and presentation of evidence

Due to the huge data generated by IoT devices (which can be referred to as 'Big IoT Data'), it is important that the research community finds a way to create techniques that are smart to analysis the data. This data is generated from heterogenous devices which have vendor specific data formats that are varied making it cumbersome to analyse and produce reports that are admissible in a court of law when presented.

3) Provision of forensic readiness

The production of IoT equipment and provision of IoT services that are readily adaptable and integrated into the current digital processes is still a challenge in digital forensics investigations. Even though measures have been taken to address security features in IoT, issues related to forensics readiness for IoT systems still remain clouded [59].

4) Mitigating the privacy risks

Privacy is a contentious issue in relation to investigation processes that involve personal and protected data as stipulated under the EU data protection laws and General Data Protection Regulations (GDPR). Full disclosure must be given to the owners. This involves letting them know that their data will be used for the investigation process and should be made aware of how the data was accessed and by whom. Those who access the data must put in place protective measures that forbids unauthorised access, any form of manipulation and loss.

5) Solutions to resolve legal issues

Evidence admissibility in a key issue in digital forensics, however, many of the models discussed in this survey have not addressed the legal aspects related to how evidence is acquired. The challenges relating to cross-border jurisdictions are imminent in cloud forensics which is huge part of IoT systems. There needs to be propositions for solutions for legal challenges as IoT relies heavily on the cloud both for application services and architectural structure.

6) The need for digital warrants

As evidenced by both NBT and LoS algorithm models, it is difficult to determine the scope of the investigation. This is because, potentially new evidence sources are likely to be found during the process of the investigation. With the challenges related to limited visibility and high volatility of the data exposing it to manipulation and compromise, it calls for the need for mechanisms that are practical. This can be resolved by the implementation of digital warrants which would help to effectively retrieve evidence from sources that are discovered later in the process or along the process.

VIII. CONCLUSION

As a fast-growing technology, IoT is providing the much-needed convenience to people through innovative IoT based applications. This has enabled devices to be connected in large numbers thereby sharing data with each other. Hackers have taken advantage of this data sharing capability exploited vulnerabilities leading to criminal activities. Through digital forensics solutions, these hackers can be tracked down and the causes of the attacks identified for appropriate actions to be taken.

The process of data acquisition in IoT environment continues to be a challenge and this gives rise to opportunities for research communities to develop new digital forensics methodologies, techniques, and tools. With the increase of attacks related to IoT, there is a massive need for successful prosecution of perpetrators.

The current models and frameworks have laid a building block for future work that should be more practical and experimental. As this SLR reveals, there is a need for development of intelligent and more efficient tools that are scientifically validated to ensure reliable guiding procedures leading to successful digital investigations in IoT environments.

REFERENCES

[1] I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. M. A. Kazmi, and C. S. Hong, 'Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges', *Futur. Gener. Comput. Syst.*, vol. 92, pp. 265–275, Mar. 2019.

[2] T. hoon Kim, C. Ramos, and S. Mohammed, 'Smart City and IoT', *Future Generation Computer Systems*, vol. 76, North-Holland, pp. 159–162, 01-Nov-2017.

[3] Cisco, ‘At-a-Glance Connected Means Informed’, 2016.

[4] E. Al-Masri, Y. Bai, and J. Li, ‘A Fog-Based Digital Forensics Investigation Framework for IoT Systems’, *2018 IEEE Int. Conf. Smart Cloud*, pp. 196–201, Sep. 2018.

[5] H. HaddadPajouh, A. Dehghantanha, R. Khayami, and K. K. R. Choo, ‘A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting’, *Futur. Gener. Comput. Syst.*, vol. 85, pp. 88–96, Aug. 2018.

[6] V. R. Kebande and I. Ray, ‘A generic digital forensic investigation framework for Internet of Things (IoT)’, in *Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016*, 2016, pp. 356–362.

[7] M. Chernyshev, S. Zeadally, Z. Baig, and A. Woodward, ‘Internet of things forensics: The need, process models, and open issues’, *IT Prof.*, vol. 20, no. 3, pp. 40–49, May 2018.

[8] V. S. Harichandran, F. Breitinger, I. Baggili, and A. Marrington, ‘A cyber forensics needs analysis survey: Revisiting the domain’s needs a decade later’, *Comput. Secur.*, vol. 57, pp. 1–13, 2016.

[9] M. Harbawi and A. Varol, ‘An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework’, in *2017 5th International Symposium on Digital Forensic and Security, ISDFS 2017*, 2017, pp. 1–6.

[10] L. Babun, A. K. Sikder, A. Acar, and A. S. Uluagac, ‘IoTDots: A Digital Forensics Framework for Smart Environments’, 2018.

[11] S. Zawoad and R. Hasan, ‘FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things’, in *Proceedings - 2015 IEEE International Conference on Services Computing, SCC 2015*, 2015, pp. 279–284.

[12] C. Hauser, ‘In Connecticut Murder Case, a Fitbit Is a Silent Witness’, *New York Times*, 2017. [Online]. Available: https://www.nytimes.com/2017/04/27/nyregion/in-connecticut-murder-case-a-fitbit-is-a-silent-witness.html. [Accessed: 14-Jul-2020].

[13] R. C. Hegarty, D. J. Lamb, and A. Attwood, ‘Digital evidence challenges in the internet of things’, *10th Int. Netw. Conf. INC 2014*, pp. 163–172, 2014.

[14] B. Kitchenham, ‘Guidelines for performing Systematic Literature Reviews in Software Engineering’, *Softw. Eng. Gr. Sch. Comput. Sci. Math.*, p. 65, 2007.

[15] X. Feng and Y. Zhao, ‘Digital forensics challenges to big data in the cloud’, in *Proceedings - 2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, iThings-GreenCom-CPSCom-SmartData 2017*, 2018, vol. 2018-Janua, pp. 858–862.

[16] S. Alabdulsalam, K. Schaefer, T. Kechadi, and N. A. Le-Khac, ‘Internet of things forensics – Challenges and a case study’, in *IFIP Advances in Information and Communication Technology*, 2018, vol. 532, pp. 35–48.

[17] A. D. Cartier, D. H. Lee, B. Kantarci, and L. Foschini, ‘IoT-big data software ecosystems for smart cities sensing: challenges, open issues, and emerging solutions’, in *Communications in Computer and Information Science*, 2018, vol. 707, pp. 5–18.

[18] Á. Macdermott, T. Baker, and Q. Shi, ‘Iot Forensics: Challenges for the Ioa Era’, in *2018 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018 - Proceedings*, 2018, vol. 2018-Janua, pp. 1–5.

[19] I. Walden, ‘Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent’, Springer, London, 2013.

[20] H. Jahankhani and A. Hosseinian-Far, ‘Challenges of cloud forensics’, in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017, vol. 10131 LNCS, pp. 1–18.

[21] D. Birk and C. Wegener, ‘Technical issues of forensic investigations in cloud computing environments’, in *2011 6th IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, SADFE 2011*, 2011, pp. 1–10.

[22] A. Venčkauskas, R. Damaševičius, V. Jusas, J. Toldinas, D. Rudzika, and G. Drėgvaitė, ‘A REVIEW OF CYBER-CRIME IN INTERNET OF THINGS: TECHNOLOGIES, INVESTIGATION METHODS AND DIGITAL FORENSICS’, *Int. J. Eng. Sci. Res. Technol.*, vol. 4, no. 10, pp. 460–477, Feb. 2015.

[23] P. H. Rughani, ‘IoT Evidence Acquisition – Issues and Challenges’, *Res. India Publ.*, vol. 10, no. 5, pp. 1285–1293, 2017.

[24] P. Eden *et al.*, ‘SCADA System Forensic Analysis Within IIoT’, Springer, Cham, 2017, pp. 73–101.

[25] V. Varadharajan and S. Bansal, ‘Data Security and Privacy in the Internet of Things (IoT) Environment’, Springer, Cham, 2016, pp. 261–281.

[26] C. Huang, R. Lu, and K. K. R. Choo, ‘Vehicular Fog Computing: Architecture, Use Case, and Security and Forensic Challenges’, *IEEE Commun. Mag.*, vol. 55, no. 11, pp. 105–111, Nov. 2017.

[27] M. Underwood, ‘Big Data Complex Event Processing for Internet of Things Provenance: Benefits for Audit, Forensics, and Safety’, in *Cyber Assurance for the Internet of Things*, Hoboken, NJ, USA: John Wiley & Sons, Inc., 2016, pp. 209–223.

[28] W. K. Hon, C. Millard, and J. Singh, ‘Twenty Legal Considerations for Clouds of Things’, Jan. 2016.

[29] M. M. Losavio, K. P. Chow, A. Koltay, and J. James, ‘The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security’, *Secur. Priv.*, vol. 1, no. 3, p. e23, May 2018.

[30] O. Adjei, N. Babu C, and O. Yakubu, ‘A REVIEW OF DIGITAL FORENSIC CHALLENGES IN THE INTERNET OF THINGS (IOT)’, *Int. J. Mech. Eng. Technol.*, vol. 9, no. 1, pp. 915–923, 2018.

[31] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, ‘Internet of Things Forensics: Challenges and Approaches’, in *Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, 2013, pp. 608–615.

[32] S. Perumal, N. Md Norwawi, and V. Raman, ‘Internet of Things(IoT) digital forensic investigation model: Top-down forensic approach methodology’, in *2015 5th International Conference on Digital Information Processing and Communications, ICDIPC 2015*, 2015, pp. 19–23.

[33] V. R. Kebande *et al.*, ‘Towards an integrated digital forensic investigation framework for an IoT-based ecosystem’, in *Proceedings - 2018 IEEE International Conference on Smart Internet of Things, SmartIoT 2018*, 2018, pp. 93–98.

[34] K. M. S. Rahman, M. Bishop, and A. Holt, ‘Internet of Things Mobility Forensics’, in *Proceedings of the 2016 Information*

Security Research and Education (INSuRE) Conference (INSuRECon-16), 2016, no. September, pp. 1–7.

[35] J. H. Ryu, S. Y. Moon, and J. H. Park, 'The study on data of smart home system as digital evidence', in *Lecture Notes in Electrical Engineering*, 2018, vol. 474, pp. 967–972.

[36] M. Banday, 'Enhancing the security of IOT in forensics', in *2017 International Conference on Computing and Communication Technologies for Smart Nation, IC3TSN 2017*, 2018, vol. 2017-Octob, pp. 193–198.

[37] V. R. Kebande, N. M. Karie, and H. S. Venter, 'Cloud-Centric Framework for isolating Big data as forensic evidence from IoT infrastructures', in *2017 1st International Conference on Next Generation Computing Applications, NextComp 2017*, 2017, pp. 54–60.

[38] A. Nieto, R. Rios, and J. Lopez, 'A Methodology for Privacy-Aware IoT-Forensics', in *2017 IEEE Trustcom/BigDataSE/ICESS*, 2017, pp. 626–633.

[39] V. R. Kebande, N. M. Karie, and H. S. Venter, 'Adding Digital Forensic Readiness as a Security Component to the IoT Domain', *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 1, p. 1, 2018.

[40] M. Hossain, Y. Karim, and R. Hasan, 'FIF-IoT: A forensic investigation framework for IoT using a public digital ledger', in *Proceedings - 2018 IEEE International Congress on Internet of Things, ICIOT 2018 - Part of the 2018 IEEE World Congress on Services*, 2018, pp. 33–40.

[41] M. Hossain, R. Hasan, and S. Zawoad, 'Probe-IoT: A public digital ledger based forensic investigation framework for IoT', in *INFOCOM 2018 - IEEE Conference on Computer Communications Workshops*, 2018, pp. 1–2.

[42] G. Dorai, S. Houshmand, and I. Baggili, 'I Know What You Did Last Summer', in *Proceedings of the 13th International Conference on Availability, Reliability and Security - ARES 2018*, 2018, pp. 1–10.

[43] D. Quick and K. K. R. Choo, 'IoT Device Forensics and Data Reduction', *IEEE Access*, vol. 6, pp. 47566–47574, 2018.

[44] N. H. Nik Zulkipli, A. Alenezi, and G. B. Wills, 'IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things', in *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security*, 2017, pp. 315–324.

[45] C. Shin, P. Chandok, R. Liu, S. J. Nielson, and T. R. Leschke, 'Potential forensic analysis of IoT data: An overview of the state-of-the-art and future possibilities', in *Proceedings - 2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, iThings-GreenCom-CPSCom-SmartData 2017*, 2018, vol. 2018-Janua, pp. 705–710.

[46] M. B. Al-Sadi, L. Chen, and R. J. Haddad, 'Internet of Things Digital Forensic Investigation Using Open Source Gears', in *Conference Proceedings - IEEE SOUTHEASTCON*, 2018, vol. 2018-April, pp. 1–5.

[47] F. Bouchaud, G. Grimaud, and T. Vantroys, 'IoT Forensic', in *Proceedings of the 13th International Conference on Availability, Reliability and Security - ARES 2018*, 2018, vol. 9, pp. 1–9.

[48] A. Goudbeek, K. K. R. Choo, and N. A. Le-Khac, 'A Forensic Investigation Framework for Smart Home Environment', in *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, 2018, pp. 1446–1451.

[49] C. M. Rondeau, M. A. Temple, and J. Lopez, 'Industrial IoT cross-layer forensic investigation', *Wiley Interdiscip. Rev. Forensic Sci.*, vol. 1, no. 1, p. e1322, Jan. 2018.

[50] M. Hossain, R. Hasan, and S. Zawoad, 'Trust-IoV: A trustworthy forensic investigation framework for the internet of vehicles (IoV)', in *Proceedings - 2017 IEEE 2nd International Congress on Internet of Things, ICIOT 2017*, 2017, pp. 25–32.

[51] D. P. Le, H. Meng, L. Su, S. L. Yeo, and V. Thing, 'BIFF: A Blockchain-based IoT Forensics Framework with Identity Privacy', in *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, 2019, vol. 2018-Octob, pp. 2372–2377.

[52] E. Oriwoh and P. Sant, 'The forensics edge management system: A concept and design', in *Proceedings - IEEE 10th International Conference on Ubiquitous Intelligence and Computing, UIC 2013 and IEEE 10th International Conference on Autonomic and Trusted Computing, ATC 2013*, 2013, pp. 544–550.

[53] H. Chi, T. Aderibigbe, and B. C. Granville, 'A Framework for IoT Data Acquisition and Forensics Analysis', in *Proceedings - 2018 IEEE International Conference on Big Data, Big Data 2018*, 2019, pp. 5142–5146.

[54] C. Meffert, D. Clark, I. Baggili, and F. Breitinger, 'Forensic State Acquisition from Internet of Things (FSAIoT)', in *Proceedings of the 12th International Conference on Availability, Reliability and Security - ARES '17*, 2017, vol. 11, pp. 1–11.

[55] T. Zia, P. Liu, and W. Han, 'Application-Specific Digital Forensics Investigative Model in Internet of Things (IoT)', in *Proceedings of the 12th International Conference on Availability, Reliability and Security - ARES '17*, 2017, pp. 1–7.

[56] D. Quick and K. K. R. Choo, 'Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+OSINT): A timely and cohesive mix', *Futur. Gener. Comput. Syst.*, vol. 78, pp. 558–567, Jan. 2018.

[57] N. Koroniotis, N. Moustafa, E. Sitnikova, and J. Slay, 'towards developing network forensic mechanism for botnet activities in the IoT based on machine learning techniques', in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, 2018, vol. 235, pp. 30–44.

[58] G. S. Chhabra, V. P. Singh, and M. Singh, 'Cyber forensics framework for big data analytics in IoT environment using machine learning', *Multimedia Tools and Applications*, Springer US, pp. 1–20, 13-Jul-2018.

[59] E. Bajramovic, K. Waedt, A. Ciriello, and D. Gupta, 'Forensic readiness of smart buildings: Preconditions for subsequent cybersecurity tests', in *IEEE 2nd International Smart Cities Conference: Improving the Citizens Quality of Life, ISC2 2016 - Proceedings*, 2016, pp. 1–6.