Navigating the Complex Landscape of IoT Forensics: Challenges and Emerging Solutions

Nura Shifa Musa
College of Engineering, Al Ain University, UAE
nura.shifa@aau.ac.ae

Nada Masood Mirza
College of Engineering, United Arab Emirates University, UAE
nada.mirza@uaeu.ac.ae

Adnan Ali
Al Ain, UAE
adnan14711@gmail.com

Abstract: *With the increasing proliferation of the Internet of Things (IoT) devices, digital forensics professionals face numerous challenges while investigating cybercrimes. The vast number of IoT devices, the heterogeneity of their formats, and the diversity of the data they generate make identifying and collecting relevant evidence a daunting task. This research paper explores the complex landscape of IoT forensics, highlighting the major challenges and emerging solutions. We start by listing the available digital forensics models and frameworks. We then delve into evidence management during IoT forensic investigation stages such as Identification, Acquisition, Preservation and Protection, Analysis and Correlation, Attack and Deficit Attribution and lastly, Presentation. Furthermore, we highlight the current challenges, open issues and major security and privacy concerns related to IoT forensics. Finally, we review state-of-the-art IoT forensics, exploring the possible solutions proposed in recent literature. Overall, this paper provides a comprehensive overview of the current IoT forensics ecosystem and the challenges and proposes the latest possible solutions, which are critical for ensuring the security and integrity of IoT-enabled critical infrastructures and can serve as a valuable resource for researchers and practitioners in the field.*

Keywords: *Digital forensic, internet of things, internet of things forensics, forensic investigation process, challenges, emerging solutions.*

Received April 1, 2023; accepted May 10, 2023
https://doi.org/10.34028/iajit/20/3A/7

1. Introduction

Digital Forensics (DF) may be defined as the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody [3].

The Internet of Things (IoT) refers to systems that involve computation, sensing, communication, and actuation [38]. Over the past few years, the IoT has revolutionized the connection between humans, non-human physical objects, and cyber objects, enabling monitoring, automation, and decision-making. Nowadays, several elite services are accessible by people over the IoT, which is a heterogeneous network defined by machine-to-machine communication [16]. There are many IoT-based domains such as, but not limited to, Smart Cities [10], Smart Homes [20], Health Care [31], and Agriculture [30]. The Internet of Things can be important in aiding the forensic investigation process. It opens up doors of opportunity by offering digital traces since it is linked to many devices. These digital traces can give investigators a lot of information that can either prove or disprove their theories. This could help the professionals find answers and recreate the crime scene.

Digital forensics has faced many legal and technological challenges with this rapid base growth and a paradigm shift away from conventional standalone devices. Studies reveal that applying traditional DF tools is no longer useful or applicable [41]. Furthermore, IoT devices do not currently have any standard method to collect evidence forensically soundly [23].

As IoT Forensics is a big area of study, numerous papers have been conducted previously on various topics related to digital forensics. However, only a few provided a comprehensive overview of the complex IoT Forensics ecosystem, such as [6, 38]. Additionally, several other important aspects of IoT forensics discussed in the current study have not been previously reported. The contributions of this study are as follows:

- Investigating the state-of-the-art research on IoT forensics
- Providing a simple, concise and comprehensive overview of the current complex IoTF ecosystem
- Classifying the research papers by devising a taxonomy that reflects the latest IoTF literature
- Exploring evidence management requirements for each IoT Forensic Investigation phase
- Identifying and comparing different IoT forensics Investigation modes
- Addressing current security and privacy concerns related to IoT forensics
- Listing the latest promising solutions in overcoming digital forensics challenges

This paper aims to shed light on Navigating the Complex Landscape of IoT Forensics Challenges and Emerging Solutions. First, IoT Forensics theoretical frameworks are discussed. Fundamental challenges during the forensic investigation process are identified and later explored; the latest promising technologies that can aid in overcoming digital forensics challenges such as Deep Learning, Fog computing, Blockchain, DNA and Genes, Logging Scheme, Quantum Cryptography, HFIoTS, Digital Twin Technology and IoT Honeypot in IoT Forensics. The scope of the research paper is identified by the below IoTF Taxonomy (Figure 1).

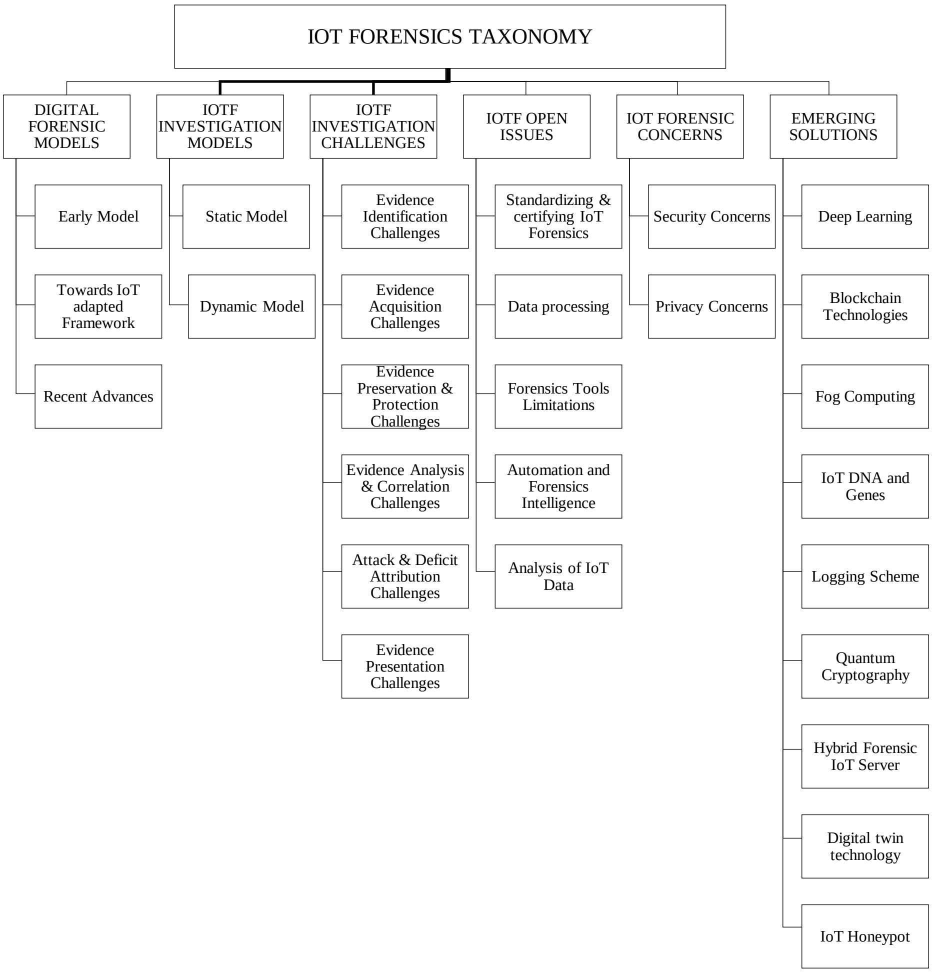
IOT FORENSICS TAXONOMY
DIGITAL FORENSIC MODELS
Early Model
Towards IoT adapted Framework
Recent Advances
IOTF INVESTIGATION MODELS
Static Model
Dynamic Model
IOTF INVESTIGATION CHALLENGES
Evidence Identification Challenges
Evidence Acquisition Challenges
Evidence Preservation & Protection Challenges
Evidence Analysis & Correlation Challenges
Attack & Deficit Attribution Challenges
Evidence Presentation Challenges
IOTF OPEN ISSUES
Standardizing & certifying IoT Forensics
Data processing
Forensics Tools Limitations
Automation and Forensics Intelligence
Analysis of IoT Data
IOT FORENSIC CONCERNS
Security Concerns
Privacy Concerns
EMERGING SOLUTIONS
Deep Learning
Blockchain Technologies
Fog Computing
IoT DNA and Genes
Logging Scheme
Quantum Cryptography
Hybrid Forensic IoT Server
Digital twin technology
IoT Honeypot

Figure 1. Internet of things forensics taxonom.

2. Related Work

There are various pieces of research on IoT Forensics. Some of the research are summarized below:

A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues by Stoyanova *et al*. [38] Has aimed to present a comprehensive survey on IoT Forensics. After introducing the necessary terminologies, specifications, and clarifications, Stoyanova et al. presented the current challenges based on the digital forensic investigation processes: identification, acquisition, evidence analysis, correlation, attack/deficit attribution, and presentation. The authors also summarized the IoT Forensics models' evolution over the years. The three main sections of DF Process Models are Early Models (1995-2005), Towards IoT Adopted Framework (2005-2015), and Recent Advances (2016-2019) (See Table 1). It mentioned popular frameworks like the 1-2-3-Zones approach and other, more recent frameworks that leverage the Internet of Things to collect evidence without violating the user's privacy rights. It also gave a brief overview of the video-based evidence analysis framework and the use of the blockchain framework in the forensics investigation process. Finally, the survey highlights some open issues in IoT forensics, such as standardization, forensic tool limitations, automation, and forensic intelligence.

Table 1. Previous research on the digital forensics process models.

Digital Forensics Process Models	Author	Year
Scientific Crime Scene Investigation (SCSI) Model	Lee *et al*. [24]	2001
End To End Digital Investigation (EEDI)	Stephenson [37]	2003
Hierarchical Objectives-based Framework	Beebe and Clark [8]	2005
Common Process Model for Incident Response (IR) and Forensics	Freiling and Schwittay [13]	2007
Multi-component View of Digital Forensics	Grobler *et al*. [14]	2010
Digital Forensics as a Service	Van Baar *et al*. [40]	2014
Application-Specific Digital Forensics Investigative Model in IoT	Zia *et al*. [43]	2017
Digital forensics model of smart city automated vehicles challenges.	Feng *et al*. [12]	2017
A comprehensive micro unmanned aerial vehicle (UAV/Drone) forensic framework	Jahan *et al*. [32]	2019

Xiao *et al*. [41] developed advanced forensic video analysis techniques to aid forensic investigation in Video-Based Evidence Analysis and Extraction in Digital Forensic Investigation. After introducing the necessary terminology specifications and clarifications, Xiao *et al*. [41] addressed the challenges in obtaining evidence from low-quality footage. They proposed two enhancement algorithms: Adaptive Histogram Equalization (AHE) and contrast-limited AHE (CLAHE). The authors also proposed an object identification technique based on deep learning. This highly intelligent technique can easily identify the objects in the footage. In conclusion, Xiao et al. developed a way to ensure that video quality can be enhanced to extract as much evidence as possible. It suggested a methodology to collect more evidence items in a reverse manner.

Kumar *et al*. [23] In an Internet-of-Forensic (IoF): A blockchain-based digital forensics framework for IoT applications aims to propose a blockchain-based framework tailored for IoT applications. This platform provides a transparent view for all participants during the investigation process. After introducing the necessary terminologies, specifications, and clarifications. Kumar *et al*. [23] proposed a framework that relies on blockchain and IoT for evidence gathering and communications. The proposed framework uses consortium blockchain to facilitate cross-border investigation.

Moreover, to provide a security feature for blockchain, lattice-based cryptography is implemented to defend against quantum computing attacks. The method was effective in complexity, time, memory and CPU use, gas use, and energy analysis.

Al-Masri *et al*. [3] proposed a Fog-Based Digital Forensics Investigation Framework that addresses the challenges related to IoT forensics, from computing power to data filtering to data aggregation. Therefore, a fog computing solution can overcome devices' processing and memory limitations while defending the IoT system against cyber-attacks. Lastly, by analyzing the data with the framework, the authors could detect suspicious activities that would notify other nodes. This will prevent the threat from propagating to other IoT devices and limit cyber-attack spread.

Khanpara *et al*. [21], Explored IOTF through data analytics lenses. The paper listed several tools developed to assist investigators in real-time collection and processing, such as Encase, RegRipper, FTK (Forensic ToolKit) and computer-aided investigative environment (CAINE).

3. Digital Forensics Model Overview

In forensics, the term “model” refers to the theoretical representation of the investigative process, while a “framework” implies a practical implementation of these processes [17]. Stoyanova *et al*. [38]. Broke down their research on the process model into three sections:

3.1. Early Models (1995-2005)

Early models contained several proposed approaches with basic digital forensics concepts even before the IoT paradigm was born and have greatly contributed to the frameworks' evolution.

3.2. Towards IoT adopted Framework (2005-2015)

During this time frame, more advanced proposed approaches that outlined some of the most well-established models were implemented. Below are some highlighted models:

The Three Zones Approach by Oriwoh *et al*. [28]. It is the most popular theoretical framework in DF science, and it divides IoT forensics into three main areas:

- Zone One: It includes physical parts, software, and networks.
- Zone two joins the internal and external zones, covering intrusion detection and prevention systems and devices.
- Zone Three: It covers cloud, services gateway, or edge devices not connected to the network.

The Next-Best-Thing Triage Model by Oriwoh [29] approach assists the investigator in obtaining evidence of a crime. It identifies the device that generates the data even if it's physically unavailable. This framework can also be combined with other forensic models and frameworks.

A Forensics-Aware Model for the IoT (FAIoT) was proposed by Zawoad and Hasan [42]. The goal of FAIoT is to use a centralized repository in an IoT environment and make sure that the evidence collected is valid and reliable so that it can be analyzed.

3.3. Recent Advances (2016-2019)

Despite relatively new IoT forensics, some potential models have already been developed. Below are some highlighted models:

A Digital Forensics Investigation Framework (DFIF-IoT*)* was discussed in 2016 by Kebande and Ray [19]. A major advantage of this approach is that it complies with ISO/IEC 27043: An Integrated Digital Forensics Investigation Framework. This model can look at potential digital evidence (PDE) made by an ecosystem based on the Internet of Things.

The Last-on-Scene (LoS) Algorithm by Harbawi and Varol [15]. This approach provided an improved theoretical framework for IoT forensics, addressing the challenges of evidence acquisition. According to Harbawi and Varol's LoS Algorithm, the last device in the communication chain must be examined first. Thus, this approach limits the scope of the investigation.

Privacy-Aware IoT Forensics [34]. Extracting evidential data without compromising users' privacy rights could be exceptionally hard in IoT settings. By implementing the

ISO/IEC 29100:2011 regulation across the entire forensic investigation process,

Nieto *et al*. [26] Established a model (PRoFIT) that considers privacy regulations. The suggested framework emphasizes the need to work with surrounding devices to acquire information and reconstruct the context of the crime scene.

4. IoT Forensic Investigation Process

As the use of IoT devices continues to grow, the importance of IoT forensics will only increase. To properly investigate IoT-related crimes, investigators must be adequately trained on following proper procedures and understand evidence management in a forensically sound manner throughout all stages of the forensic investigation, from evidence Identification, Acquisition, Preservation and Protection, Analysis and Correlation, Attack and Deficit Attribution to Presentation. To ensure the integrity and admissibility of evidence in court [25, 33].

4.1. Evidence Identification

Identification of evidence is the first step in the process of IoT forensics. IoT devices generate vast amounts of data, and knowing what to look for when investigating an incident is essential. Evidence identification can involve locating and documenting the device and its components and analyzing network traffic and log files for anomalies [35].

4.2. Evidence Acquisition

Once the evidence has been identified, it must be acquired forensically to maintain its integrity and admissibility in court. IoT devices can be challenging to acquire evidence from, as they often have limited storage and constantly generate new data. It is crucial to use specialized tools and techniques to acquire evidence from IoT devices without altering or damaging them [39].

4.3. Evidence Preservation and protection

Preservation and protection of evidence are vital to maintaining the integrity of the evidence. Any alteration or damage to evidence can lead to its inadmissibility in court. Proper procedures for handling and storing evidence can help ensure it is not tampered with or lost. Each piece of evidence should be given a specific reference number and described [9].

4.4. Evidence Analysis and Correlation:

Evidence analysis and correlation involve examining and interpreting the acquired data to determine its relevance to the case. This step requires specialized knowledge and tools to analyze the vast amounts of data IoT devices generate. The correlation of different evidence pieces can help build a timeline of events and identify potential suspects [4].

4.5. E. Attack and Deficit Attribution

The fifth step in IoT forensic investigation is attack and deficit attribution. It involves identifying the cause of the attack and attributing the deficit to the responsible party. In this phase, investigators use the collected evidence to determine the type of attack used and who was responsible for the attack. Attribution is essential as it helps investigators bring the responsible party to justice and prevent future attacks [18].

4.6. Evidence Presentation

The presentation of evidence is the final step in IoT forensics. The evidence must be presented clearly and concisely, which is understandable by both technical and non-technical personnel. The presentation of evidence can include visual aids, such as graphs and charts, to help illustrate the data and its relevance to the case.

5. IoT Forensic Investigation Modes

A digital forensic investigation can be performed using two modes of analysis: static and dynamic. In this section, we will discuss the difference between these two modes of analysis and highlight their respective advantages and limitations. Understanding these differences is critical to ensure that the correct mode of analysis is employed in a given investigation. A skilled forensic investigator should be able to weigh the benefits and drawbacks of each mode of analysis and determine the most appropriate approach for the investigation at hand [2].

5.1. Static Analysis

Static analysis is a traditional forensic investigation technique that involves examining data at rest, i.e., examining data acquired from a digital device and no longer actively running. The analysis is performed on a forensic image, an exact copy of the digital device's storage media, created using specialized software. During static analysis, the forensic investigator typically searches for artifacts that may provide evidence of the digital device's usage, such as deleted files, browser history, and chat logs. This mode of analysis is particularly useful when the investigator is interested in the historical data on a device as opposed to the current state of the device. However, static analysis has limitations, including the inability to capture real-time information or encrypted data.

5.2. Dynamic Analysis

On the other hand, dynamic analysis involves analyzing a digital device while it is actively running. This mode of analysis captures real-time information and can provide valuable insights into the device's current state. For example, dynamic analysis can capture network activity, running processes, and system configuration settings not stored in the forensic image. Dynamic analysis can be performed using specialized software that allows the investigator to capture the device's memory or RAM. This type of analysis is particularly useful when investigating malware or other types of malicious software that may be actively running on a device. However, the dynamic analysis also has some limitations, including the potential for data loss if the investigator is not careful with the tools used to capture the device's memory.

6. Current Challenges In IoT Forensics

The National Institute of Standards and Technology (NIST) outlines cloud and IoT forensics issues. All major concerns were classified into six broad categories:

6.1. Evidence Identification

1. Scope of the Compromise and Reconstruction of the Crime Scene: Due to the volatile nature of communication, reconstructing the crime scene and assessing the extent of the damage is quite challenging in the IoT environment.
2. Data Proliferation: Examiners should filter the data and analyze what’s relevant to conduct an efficient investigation. This task is challenging as it deals with interconnected devices and raw data.
3. Data Location: It is common for IoT devices to migrate between different physical locations while operating. Hence, digital forensics professionals encounter considerable challenges when trying to locate evidence.

6.2. Evidence Acquisition

1. Inadequate Training and Poor Knowledge: first responders and investigators need proper training to obtain evidence professionally.
2. Data encryption: since storing data in an encrypted format is possible, investigators must have significant knowledge of various systems and standards to investigate any kind of IoT-related crime.

6.3. Evidence Preservation and Protection

1. *Maintaining the Chain of Custody*: since data comes from various servers, it can be difficult to track evidence movement.
2. *Lifespan Limitation*: Another issue with IoT devices is the lack of memory. The ongoing nature of the devices makes it possible for data to be overwritten, which may lead to the loss of evidence.
3. *The lack of transparency*: Cloud service providers (CSP) usually don't reveal details about their infrastructure to protect their business reputation and customer privacy
4. *Data retention:* The service provider usually determines how long data is stored.

6.4. Attack and Deficit Attribution

1. *Sharing Resources*: Cloud computing involves sharing a physical server with multiple users simultaneously. Thus, in such cases, if one user engages in illegal activity, Investigators may need to consider the services used by a single customer and the whole infrastructure.
2. *Identifying Liabilities*: Forensics examiners should verify that the locations and time settings of IoT devices were set precisely if it suggests that it was present at the crime scene. Moreover, the investigators must determine whether another person used the device simultaneously.

6.5. Evidence Analysis and Correlation

3. Evidence Analysis and Correlation: metadata like location, copyright status, creation date, and time) are not stored in the majority of IoT devices. This eliminates the possibility of correlating and logically consistent evidence obtained from multiple IoT nodes.
4. Legal Issues: Regarding cross-border crimes, there are many things to consider, such as the lack of clear procedures and legal agreements.
5. Sharing Resources: Cloud computing involves sharing a physical server with multiple users simultaneously. So, if one user does something illegal, investigators may need to look at the services used by that client and the infrastructure.
6. Identifying Liabilities: Forensics examiners should verify that IoT devices' locations and time settings were set precisely if they indicate their presence. Moreover, the investigators must determine whether another person used the device simultaneously.

6.6. Evidence Presentation

It would be difficult to explain the technicalities of cloud computing and forensics to the jury during a trial in court since the jury's basic knowledge of the complicated design comes from social media or personal knowledge.

7. Open Issues in Iot Forensics

7.1. Standardizing and certifying IoT Forensics

IoT Forensics deals with a wide range of devices and formats. With so many different people involved and technology changing so quickly, it is hard to develop a single standard.

7.2. Data Processing

In this case, the current digital forensic tools have insufficient processing speed. This occurs because some developers emphasize accuracy more than processing speed.

7.3. Forensics Tools Limitations

Commercial digital forensics tools are commonly used by investigators. A major limitation is their lack of transparency since the vendors are reluctant to share the codes of their products.

7.4. Automation and Forensics Intelligence

Using artificial intelligence for forensics has raised different ethical and social concerns. According to critics, automation could degrade the examiners' knowledge and, thus, the quality of investigations. As they move away from manual handling, the likelihood of error increases.

7.5. Analysis of IoT Data

In the IoT domain, the growth of data has exceeded the capability of traditional computing and forensics. Data complexity and processing massive amounts of information could thwart examiners from carrying out complete data analysis.

8. IOT Forensic Security and Privacy Concerns

One of the primary concerns in IoT Forensic Security and Privacy is the risk to individuals' privacy due to the ability of IoT sensors and devices to sense, collect, and transmit data over the internet. IoT Forensic Security and Privacy Concerns also include the risk of unauthorized access to data due to compromised devices. Furthermore, IoT Forensic Security and Privacy Concerns create significant implications for various businesses and public organizations, as the interconnectivity of networks in IoT introduces the accessibility from anonymous and untrusted online sources [34].

IoT Forensic Security and Privacy Concerns also arise due to insufficient data protection (communication and storage) in IoT applications. In addition, IoT devices' security vulnerabilities create opportunities for extracting traces, but criminals can also use them to undermine a device's security. IoT Forensic Security and Privacy Concerns need to be addressed to ensure the confidentiality, integrity, and availability of the data contained in the IoT devices and networks. Developing tools, technologies, methodologies, and necessary measures to secure and protect IoT devices from vulnerabilities and threats is essential. Addressing IoT Forensic Security and Privacy Concerns is critical to protect our personal information and ensuring the security of the nation's critical infrastructure.

Overall, IoT Forensic Security and Privacy Concerns are significant challenges that must be addressed in the IoT environment. The interconnectivity of networks in IoT, security vulnerabilities of IoT devices, and insufficient data protection are the primary reasons behind these concerns. Addressing these concerns is crucial to protect individuals' privacy, securing IoT devices and networks, and ensure data confidentiality, integrity, and availability [7].

9. Emerging Solution in Iot Forensics

9.1. Analysis and Extraction of Video-Based Evidence

Traditionally, investigators manually check the footage to identify evidence items based on video content. However, this method is impractical and time-consuming, particularly for huge volumes of videos. The video evidence investigation process presents several challenges to professionals. The first consideration is quality. There are several issues related to video quality, such as rescaling images as they will not reveal additional information and low-resolution photos as they have limited potential for enhancement. Another consideration is brightness. Low brightness factors can lead to errors in examining certain contents as the image may not be clear enough. Lastly, the compression feature on many digital camera systems will cause the video or image to be compressed. This will result in details being lost and the introduction of visible artifacts into the image. Hence, the image-enhanced video analysis framework was proposed [41].

This framework applies an enhancing algorithm to the videos or images either by an Adaptive Histogram Equalization (AHE) algorithm, which is suitable when we deal with images to improve the contrast, or a contrast limited AHE (CLAHE) algorithm, which eliminates over-amplification of the contrast. For video-based forensic analysis, artificial intelligence has the potential to greatly accelerate the automation of forensic investigation, making it a more effective and efficient approach. Below are the results after the application of the above framework.

This framework object identification process may play a significant role in three areas:

- Identifying objects on video surveillance that can be considered a threat.
- Identification of abnormal activities
- Identification and detection of sensitive information in video or images

9.2. A Digital Forensics Framework Based on Blockchain For IoT Applications

The framework uses Blockchain to enhance the forensics investigation process since it provides a transparent view to all parties involved regardless of location. The process consists of evidence gathering and communication through the chain of- custody and evidence chain. The framework is divided into four main layers (see Figure 2):

1. *Edge-Internet-of-Forensics*: this layer covers all devices used by the users like (smartphones and other IoT appliances), where a Lightweight signcryption process is used to ensure the security of evidence throughout the transmission into and out of the Chain of Custody (CoC).
2. *Fog- Internet-of-Forensics*: this layer covers digital forensics tools besides fog devices.
3. *Consortium- Internet-of-Forensics*: in this layer, the consortium blockchain is implemented to enable cross-border investigation, which helps investigators to collaborate and share transparent evidence processing during the investigation of IoF.
4. *Cloud Storage*: In this layer, the data from any investigation can be held in cloud storage. The blockchain can be linked to the storage to provide a custom digital forensics system [23].

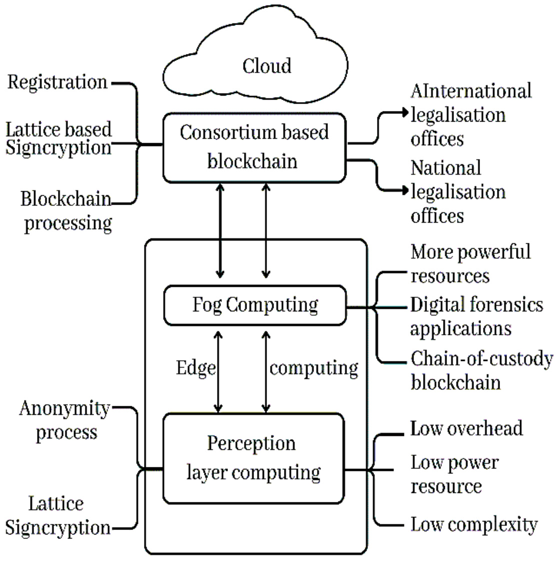
Cloud
Registration
Lattice based Signcryption
Blockchain processing
Consortium based blockchain
AInternational legalisation offices
National legalisation offices
More powerful resources
Digital forensics applications
Chain-of-custody blockchain
Fog Computing
Edge
computing
Anonymity process
Lattice Signcryption
Perception layer computing
Low overhead
Low power resource
Low complexity

Figure 2. IoF framework.

9.3. A Digital Forensics Framework Based on Fog computing For IoT Applications

A Fog-Based Investigation Framework (FoBI) is used to preserve the evidence and protect an Internet of Things (IoT) system from cyberattacks layers (see Figure 3). FoBI consists of six primary components listed below:

- Device monitoring manager
- Forensic analyzer
- Evidence recovery
- Case Reporting
- Communication
- Storage

The communication module on the FoBI allows it to communicate with IoT devices in real time when it transmits and receives data. The framework will log all the current activities through the IoT device and store them at the local storage [3].

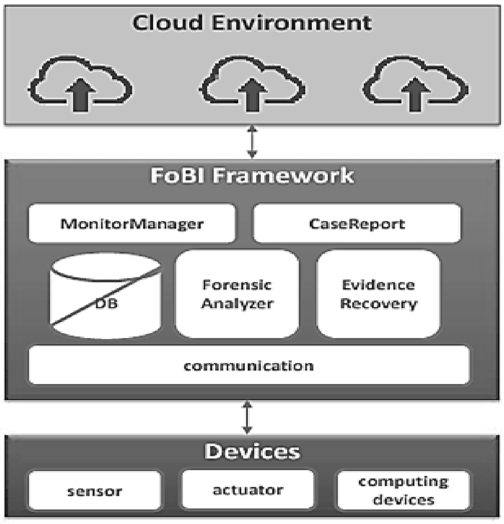

Figure 3. FoBI Framework.

9.4. DNA and Genes

In recent years, Identifying IoT devices for forensic investigation has become increasingly critical. As the use of IoT devices grows, so does the potential for cyber-enabled and dependent crime activities.

DNA and genes from devices were scientifically proven to aid the IoT forensic investigation process by identifying the IoT devices; A model of the devices' DNA is used to assign unique identification numbers to IoT devices worldwide, along with their unique attributes called genes. Among these attributes is the name of the user who purchased or registered the IoT device, the serial number of the device, and the type of device layers (see Figure 4).

Overall, using DNA and genes from IoT devices is a promising approach to identifying specific devices and their interactions with their surroundings. However, there is still much research to be done in this area to assess the efficiency and effectiveness of such a solution. Investigators must also navigate the challenges of efficiently accessing and analyzing IoT device content [35].

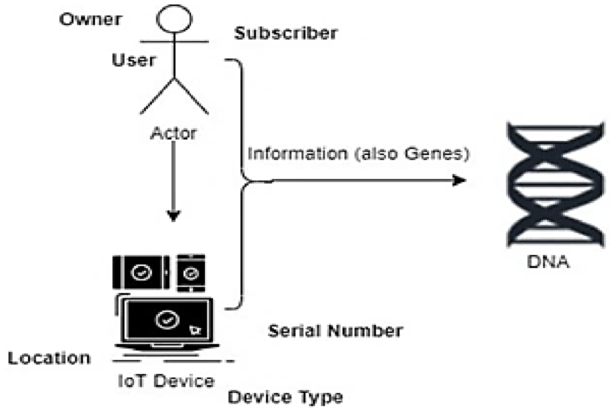

Figure 4. IoTF DNA Identification.

9.5. Logging Scheme

Through the continuous manipulation of erasing or altering information, anti-forensic tools can be frustrating for forensic professionals.

DistLog is a distributed logging scheme that aims to secure IoT log files against anti-forensics techniques. It provides a fault-tolerant and recoverable solution that effectively secures IoT devices against cyber-attacks. This solution aggregates, compresses and encrypts the logs generated by IoT devices regularly [27].

A modified information dispersal algorithm (MIDA) is then used to fragment the encrypted log files, authenticate them, and distribute them over several storage nodes to ensure they are always available. After obtaining fragments, they are sent to n neighboring IoT devices (aggregation nodes). It was demonstrated through a set of security and performance tests that the proposed solution is effective and robust at thwarting well-known security threats. Additionally, the performance analysis shows that the proposed solution has a lower computational and storage requirement than earlier works layers (see Figure 5):

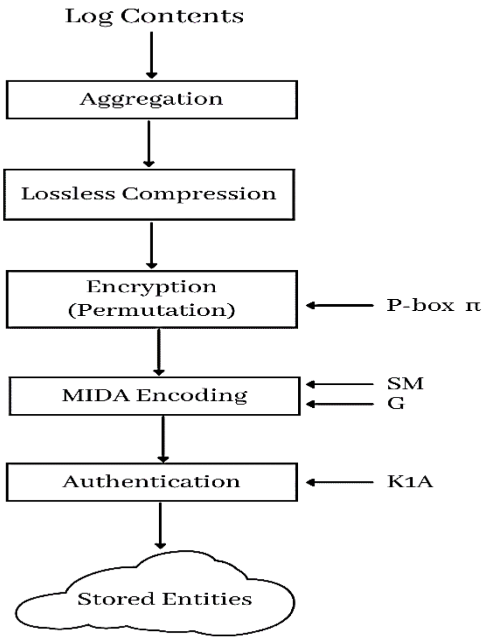

Figure 5. Proposed logs preserving scheme.

9.6. Quantum Cryptography

Quantum cryptography is a promising solution for securing the Internet of Things (IoT) and ensuring the privacy and integrity of data transmitted between IoT devices.

It can provide high security for IoT devices by using fundamental quantum properties to develop an indestructible cryptosystem. For example, quantum key distribution (QKD) allows two parties to establish a shared secret key by exchanging single photons, which cannot be intercepted or measured without altering their quantum state [5].

Researchers are actively exploring the potential of quantum cryptography for IoT forensic analysis. For example, one study proposes using post-quantum cryptography, which is resistant to attacks by classical and quantum computers, to secure IoT devices and enable forensic analysis [21]. Another study suggests using large-scale QKD technology to secure quantum protection in critical infrastructures, including IoT devices [1]. In conclusion, quantum cryptography has the potential to enhance the security of IoT devices and protect against cyber threats.

9.7. Hybrid Forensic IoT Server (HFIoTS)

Hybrid Forensic IoT Server (HFIoTS) is a system designed for the forensic analysis of Internet of Things (IoT) devices. HFIoTS integrates hardware and software components to facilitate digital evidence collection, processing, and analysis.

The hardware component of HFIoTS consists of a Raspberry Pi microcomputer that is used to acquire data from IoT devices through various interfaces such as Wi-Fi, Bluetooth, and USB. The Raspberry Pi also serves as a hub for external storage devices such as hard drives or flash drives where data can be saved.

The software component of HFIoTS is a Linux-based operating system that includes a suite of forensic tools for acquiring, analyzing, and presenting digital evidence. The software tools can extract data from IoT devices such as smartphones, smart home devices, and wearables. The data extracted can be analyzed using forensic software tools such as Autopsy, EnCase, and FTK Imager.

HFIoTS is a valuable tool for forensic investigators as it enables them to acquire digital evidence from IoT devices quickly and efficiently. The system is designed to be user-friendly and can be used by both novice and experienced investigators. The HFIoTS system can also be customized to suit the specific needs of forensic investigators, making it a versatile tool for digital forensics.

Overall, the HFIoTS system is a comprehensive solution for the forensic analysis of IoT devices that combines hardware and software components to provide a user-friendly and efficient tool for digital forensics investigations [34].

9.8. Digital twin technology

Digital twin technology can play an important role in IoT forensics by providing a virtual replica of an IoT system that can be used for forensic analysis and investigation. The digital twin captures all relevant data and information about the IoT system, including its architecture, behavior, and performance characteristics. It can simulate and test different scenarios to aid in forensic analysis.

Digital twin technology can help investigators identify and analyze potential security breaches, such as malware attacks, by comparing the behavior of the digital twin with the actual IoT system. By monitoring the digital twin for abnormal behavior or performance, investigators can identify and analyze potential threats and develop effective countermeasures. In addition, digital twin technology can be used to recreate the state of an IoT system at a particular point in time, providing valuable evidence for forensic investigations.

Another key benefit of digital twin technology in IoT forensics is its ability to provide a platform for training and testing forensic investigators. Digital twins can simulate different scenarios and provide investigators realistic training opportunities to develop their skills and expertise.

However, there are also several challenges associated with the use of digital twin technology in IoT forensics, including the need for specialized expertise and resources to develop and maintain the digital twin models, the potential for security and privacy breaches due to the sensitive nature of the data involved, and the need for ongoing maintenance and updates to ensure the accuracy and relevance of the virtual model.

Digital twin technology offers a powerful tool for IoT forensics investigations, providing a virtual replica of an IoT system that can be used for analysis, simulation, and testing. As the use of IoT devices continues to grow, digital twin technology is likely to become an increasingly important tool for forensic investigators in identifying and analyzing potential security breaches and developing effective countermeasures [11].

9.9. IoT Honeypot

IoT Honeypot or IoT trap is a type of honeypot specifically designed to detect and mitigate attacks on IoT devices. It is a software-based emulation of an IoT device designed to attract and trap attackers, allowing investigators to monitor their activities and gain insight into their methods.

IoT Honeypot emulates an IoT device’s behavior, including its network traffic, communication protocols, and other behavior patterns. When an attacker attempts to exploit the Honeypot, the device will respond with fake data or other responses designed to lure the attacker into continuing their attack. This allows investigators to observe the attacker's techniques and methods and gather evidence for forensic analysis.

IoT Honeypot can detect and analyze many attacks on IoT devices, including malware infections, phishing attempts, and other security breaches. It is particularly useful for IoT devices, which are often targeted by attackers due to their vulnerabilities and limited security features.

However, there are also several challenges associated with the use of IoT Honeypots, including the need for specialized expertise and resources to set up and maintain the honeypot, the potential for attackers to detect and evade the Honeypot, and the need for careful analysis and interpretation of the data gathered through the honeypot.

IoT Honeypot is a powerful tool for IoT forensics investigations, providing a means to trap and observe attackers and gather valuable evidence for forensic analysis. As the use of IoT devices continues to grow, IoT Honeypots and other honeypot technologies are likely to become increasingly important tools for forensic investigators in identifying and analyzing potential security breaches and developing effective countermeasures [36].

10. Conclusions

To sum up, this paper delivers an overview of the evolution of IoT forensics frameworks over the past 25 years, starting with the early models (1995-2005), which worked as a basis for IoT-adopted frameworks (2005-2015) with a focus on the recent advances and some promising models (2016 and above). Then it focused on listing common challenges that professionals face during the evidence collection in the forensic investigation process. After that, it highlighted some open issues, and lastly, it introduced some state-of-the-art solutions in employing the latest deep learning, fog computing, blockchain, DNA and Genes, Logging Scheme, Quantum Cryptography, HFIoTS, IoT Honeypot and Digital Twin Technologies in the IoT Forensics field as a game-changing panacea in this regard.

To support practical digital investigations and tackle challenges, several strategies can be employed:

- Continuing education and training: The field of digital forensics is constantly evolving, and forensic investigators must stay up-to-date with the latest technologies, techniques, and legal developments. Continuing education and training can help forensic investigators keep up with emerging challenges and maintain the necessary skills to conduct practical digital investigations.
- Collaboration: Digital forensics investigations often involve multiple stakeholders, including law enforcement, legal professionals, and technical experts. Collaboration between these stakeholders can help ensure that investigations are comprehensive, efficient, and effective.
- Standardization: Standardization of digital forensics processes and procedures can help ensure that investigations are conducted consistently and reliably. Standards can also help ensure that investigations are conducted ethically and with proper attention to privacy and data protection.
- Automation: Digital forensics investigations can be time-consuming and labor-intensive. Automating certain tasks, such as data collection and analysis, can help investigators conduct investigations more efficiently and effectively.
- International cooperation: Digital evidence is often stored in multiple jurisdictions, and international cooperation is necessary to access this evidence. International cooperation can also help investigators tackle cross-border cybercrime and other digital offenses. IoTF must be empowered at the grassroots level. Firstly, device manufacturers should support authorities by ensuring that data extracted from their products are obtained lawfully. Secondly, it's recommended to establish an international committee. This committee shall focus on updating the existing regulations and standard practices for IoT Forensics. Lastly, additional training should be provided to first responders, emphasizing protocols for handling such sensitive devices and the importance of seeking help from IT professionals, as there is a tendency to switch off the devices found at crime scenes due to a lack of knowledge, resulting in the loss of temporary data, a valuable potential source of evidence that might save resources, time and effort otherwise.

Lastly, Research and Development: Digital forensics is a rapidly evolving field, and new challenges often require new technologies and techniques.

In conclusion, this work recognizes the significance of upgrading existing forensics tools while complying with forensic procedures related to the admissibility of evidence. Although a significant amount of work has been performed in digital forensics, the volume of work done in IoTF is considered quite limited relative to its increasing complexity and rapid evolution. Research gaps indicate that most current research is more theoretical than practical. To address the aforementioned concerns, researchers and investigators must work hand in hand in developing enhanced, proactive, and standardized IoT forensics tools that can assist in the DF process. More research needs to be done in developing the above emerging solutions into frameworks that focuses on designing practical approaches to tackle the complex IoT forensics challenges at the grassroots level effectively and efficiently.

References

[1] Aguado A., Lopez V., Lopez D., Peev M., Poppe A., Pastor A., Folgueira J., Martiin V., "The Engineering of Software-Defined Quantum Key Distribution Networks," *IEEE Communications Magazine*, vol. 57, no. 7, pp. 20-26, 2019. doi: 10.1109/MCOM.2019.1800763.

[2] Alazab A., Khraisat A., and Singh S., "A Review on the Internet of Things (IoT) Forensics: Challenges, Techniques, and Evaluation of Digital Forensic Tools," Digital Forensics-Challenges and New Frontiers [Working Title]. IntechOpen, 2023. doi: 10.5772/intechopen.109840.

[3] Al-Masri E., Bai Y., and Li J., "A Fog-Based Digital Forensics Investigation Framework for Iot Systems," *in Procedings of the IEEE International Conference on Smart Cloud (SmartCloud*), New York, pp. 196-201, 2018. DOI: 10.1109/SmartCloud.2018.00040

[4] Al-Mousa M., "Generic Proactive IoT Cybercrime Evidence Analysis Model for Digital Forensics," *in Procedings of the International Conference on Information Technology*, Amman, pp. 654-659, 2021. doi: 10.1109/ICIT52682.2021.9491718.

[5] Amer O., Garg V., and Krawec W., "An Introduction to Practical Quantum Key Distribution," *IEEE Aerospace and Electronic Systems Magazine*, vol. 36, no. 3, pp. 30-55, 2021. doi: 10.1109/MAES.2020.3015571.

[6] Amiroon S. and Fachkha C., "Digital Forensics and Investigations of the Internet of Things: A Short Survey," *in Procedings of the 3rd International Conference on Signal Processing and Information Security*, Dubai, pp. 1-4, 2020. doi: 10.1109/ICSPIS51252.2020.9340150.

[7] Atlam H., Alenezi A., Alassafi M., Alshdadi A., and Wills G., "Security, Cybercrime and Digital Forensics for IoT," *Intelligent Systems Reference*

Library, pp. 551-577, 2019. doi: https://doi.org/10.1007/978-3-030-33596-0_22.

[8] Beebe N. and Clark J., "A Hierarchical, Objectives-Based Framework for The Digital Investigations Process," *Digit Investig*, vol. 2, no. 2, pp. 147-167, 2005. https://doi.org/10.1016/j.diin.2005.04.002

[9] Brotsis S., Kolokotronis N., Limniotis K., Shiaeles S., Kavallieros D., Bellini E., and Pavué C., "Blockchain Solutions for Forensic Evidence Preservation in IoT Environments," *in Procedings of the IEEE Conference on Network Softwarization (NetSoft)*, Paris, pp. 110-114, 2019. doi: 10.1109/NETSOFT.2019.8806675.

[10] Canli H. and Toklu S., "AVL Based Settlement Algorithm and Reservation System for Smart Parking Systems in IoT-based Smart Cities," *The International Arab Journal of Information Technology*,vol. 19, no. 5, pp. 793-801, 2022. https://doi.org/10.34028/iajit/19/5/11

[11] Empl P. and Pernul G., "Digital-Twin-Based Security Analytics for the Internet of Things," *Information*, vol. 14, no. 2, pp. 95, 2023. doi: https://doi.org/10.3390/info14020095.

[12] Feng X., Dawam E., and Amin S., "Digital Forensics Model of Smart City Automated Vehicles Challenges," 2017.

[13] Freiling F. and Schwittay B., "A Common Process Model for Incident Response and Computer Forensics," IMF 2007: IT-Incident Management and IT-Forensics, pp. 1-18, 2007.

[14] Grobler C., Louwrens C., and Von Solms S., "A Multi-Component View of Digital Forensics," *in Procedings of the International Conference* on Availability, Reliability, and Security, Krakow, pp. 647-652, 2010. DOI: 10.1109/ARES.2010.61

[15] Harbawi M. and Varol A.,"An Improved Digital Evidence Acquisition Model for The Internet of Things Forensic I: A Theoretical Framework," *in Proceedimgs of the 5th International Symposium on Digital Forensic and Security (ISDFS)*, Tirgu Mures, pp. 1-6, 2017. DOI: 10.1109/ISDFS.2017.7916508

[16] Houhamdi Z. and Athamena B., "Identity Identification And Management In The Internet of Things," *The International Arab Journal of Information Technology*, vol. 17, no. 4A, pp. 645-654, 2020. doi: https://doi.org/10.34028/iajit/17/4A/9

[17] Joshi R. and Pilli E., *Fundamentals of Network Forensics*, Springer, 2016.

[18] Kaushik K., Dahiya S., Bhardwaj A., and Maleh Y., *Internet of Things and Cyber Physical Systems*, CRC Press, 2022.

[19] Kebande V. and Ray I., "A Generic Digital Forensic Investigation Framework For Internet of Things," *in Procedings of the IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 356-362, Vienna, 2016. DOI: 10.1109/FiCloud.2016.57

[20] Khan M., Sajjad I., Tahir M., and Haseeb A., "IOT Application for Energy Management in Smart Homes," *Engineering Proceedings*, vol. 20, no. 1, p. 43, 2022. doi: https://doi.org/10.3390/engproc2022020043.

[21] Khanpara P., Shah I., Tanwar S., Verma A., and Sharma R., "Toward the Internet of Things Forensics: A Data Analytics Perspective," *Security and Privacy*, 2023. doi: https://doi.org/10.1002/spy2.306.

[22] Kumar A., Ottaviani C., Gill S., and Buyya R., "Securing The Future Internet of Things with Post-Quantum Cryptography," *Security and Privacy*, 2022. doi: https://doi.org/10.1002/spy2.200.

[23] Kumar G., Saha R., Lal C., and Conti M., "Internet-of-Forensic (Iof): A Blockchain-Based Digital Forensics Framework for Iot Applications," *Future Generation Computer Systems*, vol. 120, pp. 13-25, 2021.

[24] Lee H., Palmbach T., and Miller M., "Henry Lee's Crime Scene Handbook,"*Academic Press*, 2001.

[25] Mrdovic S., "IoT Forensics," *Security of Ubiquitous Computing Systems*, pp. 215-229, 2021. doi: https://doi.org/10.1007/978-3-030-10591-4_13.

[26] Nieto A., Rios R., and Lopez J., "A Methodology for Privacy-Aware IoT-Forensics," *IEEE* Trustcom/BigDataSE/ICESS, Sydney, pp. 626-633, 2017. doi: 10.1109/Trustcom/BigDataSE/ICESS.2017.293

[27] Noura H., Salman O., Chehab A., and Couturier R., "DistLog: A distributed logging scheme for IoT forensics," *Ad Hoc Networks*, vol. 98, pp. 102061, 2020, doi: https://doi.org/10.1016/j.adhoc.2019.102061.

[28] Oriwoh E. and Williams G., "Internet Of Things: The Argument for Smart Forensics," in Handbook of Research on Digital Crime, Cyberspace Security, And Information Assurance, IGI Global, pp. 407-423, 2015.

[29] Oriwoh E., Jazani D., Epiphaniou G., and Sant P., "Internet of things forensics: Challenges and Approaches," *in Procedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, pp. 608-615, 2013. DOI:10.4108/icst.collaboratecom.2013.254159

[30] Perwej Y., Haq K., Parwej F., Mumdouh M. and Hassan M., "The Internet of Things (IoT) and its Application Domains," *International Journal of Computer Applications*, vol. 182, pp. 36-49, Apr. 2019, doi: https://doi.org/10.5120/ijca2019918763.

[31] Quy V., Hau N., Anh D., and Ngoc L.,"Smart Healthcare IoT Applications Based on Fog

Computing: Architecture, Applications and Challenges," *Complex and Intelligent Systems*, vol. 8, pp. 3805-3815, 2021. doi: https://doi.org/10.1007/s40747-021-00582-9.

[32] Renduchintala A., Jahan F., Khanna R., and Javaid A., "A Comprehensive Micro Unmanned Aerial Vehicle (UAV/Drone) Forensic Framework," *Digit Investig*, vol. 30, pp. 52-72, 2019. https://doi.org/10.1016/j.diin.2019.07.002

[33] Saleh M., Othman S., Driss M., Al-dhaqm A., Ali A., Yafooz W., and Emara A., "A Metamodeling Approach for IoT Forensic Investigation," *Electronics*, vol. 12, no. 3, pp. 524, 2023. doi: https://doi.org/10.3390/electronics12030524.

[34] Scheidt N. and Adda M., "Identification of IoT Devices for Forensic Investigation," *in Procedings of the IEEE 10th International Conference on Intelligent Systems (IS)*, Varna, Bulgaria, pp. 165-170, 2020. doi: 10.1109/IS48319.2020.9200150.

[35] Scheidt N., Adda M., Chateau L., and Kutlu Y., "Forensic Tools for IoT Device Investigations in regards to Human Trafficking," *in Procedings of the IEEE International Conference on Smart Internet of Things (SmartIoT)*, Jeju, pp. 1-7, 2021. doi: 10.1109/SmartIoT52359.2021.00010.

[36] Shrivastava R., Bashir B., and Hota C., "Attack Detection and Forensics Using Honeypot in IoT Environment," *in Procedings of the Distributed Computing and Internet Technology*, Bhubaneswar, pp. 402-409, 2018. doi: https://doi.org/10.1007/978-3-030-05366-6_33.

[37] Stephenson P., "A Comprehensive Approach To Digital Incident Investigation," *Information Security Technical Report*, vol. 8, no. 2, pp. 42-54, 2003.

[38] Stoyanova M., Nikoloudakis Y., Panagiotakis S., Pallis E., and Markakis E., "A Survey on The Internet of Things (Iot) Forensics: Challenges, Approaches, and Open Issues," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 2, pp. 1191-1221, 2020.

[39] Surange G. and Khatri P., "IoT Forensics: A Review on Current Trends, Approaches and Foreseen Challenges," *in Procedings of the 8th International Conference on Computing for Sustainable Global Development*, New Delhi, pp. 909-913, 2021. DOI:10.1109/INDIACom51348.2021.00163

[40] Van Beek H., Van Eijk E., Van Baar R., Ugen M., Bodde J., and Siemelink A., "Digital Forensics as A Service: Game on," *Digit Investigation*, vol. 15, pp. 20-38, 2015. https://doi.org/10.1016/j.diin.2015.07.004

[41] Xiao J., Li S., and Xu Q., "Video-Based Evidence Analysis And Extraction In Digital Forensic Investigation," *IEEE* Access, vol. 7, pp. 55432-55442, 2019. DOI: 10.1109/ACCESS.2019.2913648

[42] Zawoad S. and Hasan R., "Faiot: Towards Building A Forensics Aware Eco System For The Internet of Things," *in Procedings of the IEEE International Conference on Services Computing*, New York, pp. 279-284, 2015. DOI: 10.1109/SCC.2015.46

[43] Zia T., Liu P., and Han W., "Application-Specific Digital Forensics Investigative Model In Internet of Things (Iot)," *in Proceedings of the 12th International Conference on Availability*, Reliability and Security, pp. 1-7, 2017. DOI:10.1145/3098954.3104052

Nura Shifa Musa is a Senior Lab Supervisor in the College of Engineering at Al Ain University (AAU), UAE. She completed her undergraduate studies in Computer Engineering at Qatar University (QU), Qatar, where she developed a strong foundation in computer science and technology. Currently, Nura is pursuing her Master's degree in the College of Information Technology at United Arab Emirates University (UAEU), UAE, specializing in the field of Information Security. With a passion for advancing cyber security measures, Nura's research interests revolve around developing innovative solutions to enhance digital security, investigating cyber threats, exploring cloud computing technology and conducting digital forensics investigations.

Nada Masood Mirza currently serves as an Instructor in the College of Engineering at United Arab Emirates University (UAEU), UAE. Ms. Nada received her BE and MS degrees in Mechatronics Engineering from the College of Electrical and Mechanical Engineering, National University of Sciences & Technology (NUST), Pakistan. Her post-graduate research was mostly focused on the application of artificial intelligence, robotics, and wireless monitoring of renewable energy systems. She worked for a few years in academia in Pakistan where her research focus was mostly on autonomous wireless intelligent robotic systems. Since 2014 she has been involved in academic activities related to control and electronics engineering in UAE.

Adnan Ali is currently working as Web Developer, UAE. He received a B. Eng. degree in Software Engineering from Al Ain University (AAU) in 2020. His graduate project and research work were mainly related to Virtual reality educational apps. He published one paper from his B. Eng. final year project. He is currently enrolled as an MS Engineering student at Universiti Sains Malaysia (USM). Research interests include Web Development, Big Data, IoT, Embedded systems and Simulation, and Virtual Reality.