Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 3, No. 5, March : 2024

IOT FORENSICS: A SURVEY ON FORENSIC PROCESS AND CHALLENGES

Manish Kumar Meher, Dept.of Computer Science and Engineering, C.V.Raman GLobal University, Bidyanagar, Mahura, Janla, Bhubaneswar, 752054, Odisha, India.
manish.meher@cgu-odisha.ac.in;

Abstract
Data security and forensics are becoming a major issue in today's era of advancement in IoT-based wireless communication networks. IoT and its many applications, particularly in industries, smart cities, smart homes, smart vehicles, and so on, communicate confidential data that helps forensic investigators investigate cybercrimes IoT devices are more susceptible to security attacks, which leads to the development of secure forensics methods. Tracking cybercrime in an IoT environment often requires investigations, for which the traditional digital forensics methodology may find it difficult to support forensic investigators due to the complexity of the Internet of Things network and the amount of data generated by that network. Advanced digital forensics frameworks and forensics tools play a major role in cybercrime investigation. This paper describes and analyzes digital forensics procedures and issues like identification, evidence-based preservation, correlation, and presentation. It uses latest literature to compare these issues. It presents a comprehensive review of current IoT forensics tools and techniques for forensics investigation. A novel forensics investigation algorithmic method is suggested.

Keywords: Cyber Forensics, IoT Forensics,Digital Forensics, Digital Forensics Tools, Digital Forensics Pro- cess,challenges in DF Process.

1 Introduction

Cyber forensics or Digital Forensics is a branch of forensic science which deals with the recovery and investigation of material found in a digital devices known as digital evidence, often associated with cyber crime.. Also it is a post forensic process which deals with the digital evidence to find out the crime and criminal involved with the crime[1].Digital Forensics is a process of collecting and analysing the data from computer systems, storage devices, and networks in a form that presented as evidence in the court.[2]. Digital forensics is the science of presenting, documenting, analyzing, preserving and identifying information and evidence of electronic and digital data from devices without hampering the user privacy. In addition, he also uses scientific techniques to reconstruct and explain the sequence of events. By assessing, examining and recording these sequences, digital forensics aims to present these illegal artefacts as evidence in court.[3] The main motive of digital forensics is to acquire and analyse data reviewed as part of a legal proceeding, while conceal, manipulate and even erase data, or target the credibility of the collected evidence is the motive of Anti-forensics techniques. [4] Digital evidence refers to the footprints left by the criminal at the compromised system can be recorded in the log files , in hard disk and any other places in the system which proves the crime and the criminal. Digital or electronic evidence is any useful information stored or transmitted in digital form that a party to a legal matter can use at trial.

2 System under Study 2.1 Digital Forensics Process

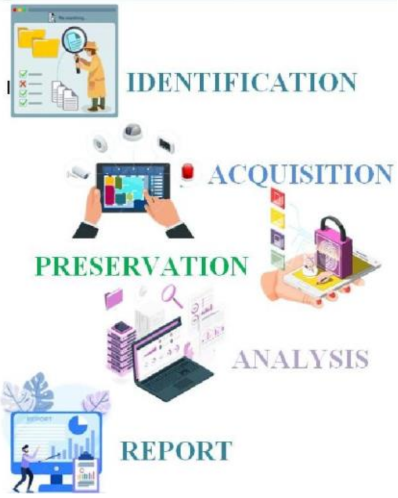


Fig. 1 Digital Forensics Process Model

The Figure 1 describe the basic five steps of the Digital forensics process which is the representation of the investigation process which represents all the steps of execution which involve identifying, acquiring, preserving, analyzing and reporting the digital evidence.

1. Identification: This step specify the identification of initial compromised device in the network and all the connected systems/device to the compromised system. Then the extraction of digital evidence from the crime related systems is carried out.
2. Acquisition : In digital forensics there is a rule of never ever work on the original evidence so in the stage of acquisition initially a duplicate copy of original digital evidence will created with which the acquisition process initiated.
3. Preservation : It is an important phase of the lifecycle where the digital evidence will transferred from the crime scene to the analysis team for farther evidence analysis. So because the digital evidence is carried out there is a chance of evidence tampering or damage. Example like the hard disk contain magnetic tape which can be got damaged if it is near to high extension line,because of the high extension line the magnetic tape will rotate automatically without power supply which cause the damage of digital evidence.
4. Analysis: In the analysis process the analysis team uses different types of authorized tools and techniques to acquire the useful digital evidence by processing and interpreting the digital evidence collected from the crime scene. Then the analysis result acquired from the evidence analysis process will be interpret for the presentation process.
5. Presentation: The presentation step deals with the preparation of the report for the result acquired from the analysis process which can be presented in the honorable court.

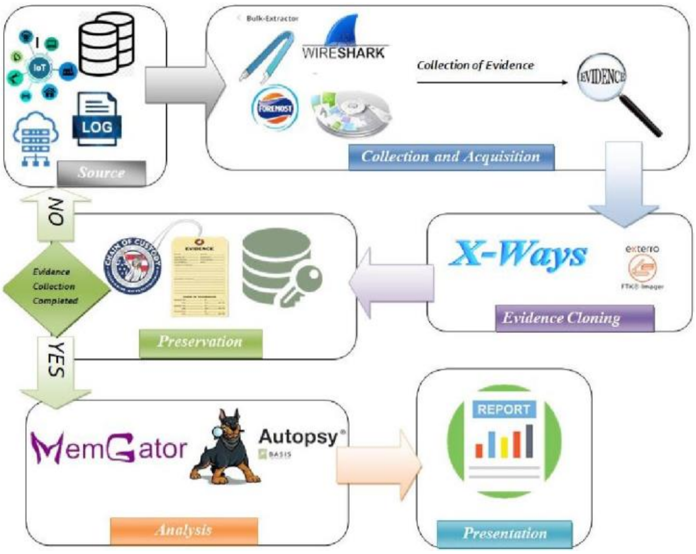


Fig. 2 IoT Forensics Working Model

Figure 2 depicts the IoT forensics working model where it shows different tools used in difference steps of the forensics process to find the digital evidence for finding the criminal Chain of custody is a documents that represents the people who have been entrusted with the evidence. It contain all the reference of all involved people, methods, tools work with the evidence everything resides with in the chain of custody.[5]

2.2 Issues in Digital Forensics Process 2.2.1 Identification:

In the field of IoT having a complex network configuration it is very difficult to find out the field of damage in the network at the time of the Identification process of Digital Forensics Investigation .

A report conducted by the International Data Corporation (IDC) states that the estimated growth of data from 2005 to 2020 is expected to be 40.000 exabytes which makes it more complicated.[6]

IoT devices are mainly design to monitor the live environment that leads to generation of tremendous amount of digital data which can be stored in multiple cloud data centres where the investigators face a major problem of gaining access to the digital evidence from multiple cloud data centres due to their security protocols .

2.2.2 Evidence Acquisition:

Rana et al. [7] also suggest That law enforcement agencies should organise training programs for their first responders in order to instruct them how to acquire digital evidence in a forensically sound manner.

The term “in a forensically sound manner” is extensively used in the Digital Forensics and implies that there must be a specific procedure applied while collecting the evidence information in order to make it usable in court [8]

Another extensive issue is the heterogeneous software and hardware specifications means due to the advancement of IoT devices different operating system and hardware are designed and introduced to design advance IoT devices. So that leads to a huge issue of evidence extract from the devices .

2.2.3 Evidence Preservation:

Suppose if the investigators are able to find the affected device which have important footprint and also gathered all the evidence , now the issue is to preserve the gathered data in such a way that it guarantees its integrity.

The term “Chain of Custody” could be defined as the accurate auditing control of original evidence material [9]. The objective of the chain of custody is to provide clean information on the timing and manner in which evidence was collected, stored, analyzed and presented. [10]. In IoT forensic maintaining the Chain of Custody while collecting evidence from multiple servers located in remote areas even complicate the process.[11]

In table 1 all the issues in IoT Forensics Process addressed by different research paper are mentioned.

SlNo.	Problem/Issues	Stoyanova et al.[1]	Alazab et al.[12]	N. Ranaet al. [13]	Hany F. Atlamet al. [14]	F. Casino etal.[15]
1	Upgradation of IoT devices to fight with cybercrime	No	No	Yes	No	Yes
2	Device and Data Proliferation	Yes	Yes	Yes	No	Yes
3	Data Location	Yes	No	No	Yes	No
4	Device Type	Yes	No	No	Yes	Yes
5	Lack of Training and Weak Knowledge Management	Yes	No	Yes	No	Yes
6	Data Encryption	Yes	Yes	Yes	Yes	Yes
7	Heterogeneous Software and/or Hardware Specifications	Yes	No	No	Yes	Yes
8	Privacy and Ethical Considerations by Accessing Personal Data	Yes	Yes	Yes	No	No
9	Lack of a Common Forensic Model in IoT	Yes	No	No	No	Yes
10	Securing the Chain of Custody	Yes	Yes	No	No	No
11	The Cloud Forensic Problem(s)	Yes	No	Yes	No	No
12	Data Protection and Lack of Transparency in Cloud Services	Yes	Yes	No	Yes	Yes
13	Data Storage	Yes	Yes	No	Yes	Yes
14	Legal Issues	Yes	Yes	No	No	Yes
15	Complexity of IoT architecture	No	Yes	No	Yes	Yes

Another is the lifespan of the IoT data because contentious generating data could easily cause data overwritten and also due to the fixed memory space causes data loss. Again there are some IoT devices that employ Real-Time Operating Systems(RTOS) and do not store the data by default[16].Again the protection of data and the transparency in the cloud service is a issue in the forensics investigation although the data is kept in different countries gaining access to those data from the data centres or to gain the access to case –related information will be governed by the laws of the country is a challenge at the time of forensics investigation .

2.2.4 Evidence Analysis and Correlation

This stage involves a thorough systematic search for evidence relating to the alleged crime and identifying importance, piecing together data fragments and making evidence-based conclusions.[17] The most of the IoT devices do not store any meta-data like time stamp , modification information etc which leads to the difficulties in the evidence collection by the investigation team .

2.2.5 Evidence Presentation:

In the evidence presentation the evidence will be presented to the panel called voir dire those who have a minimal knowledge about cloud computing and forensics at that time to describe the evidence from a technical way to in a simpler way can change the actual meaning of evidence.

3 Existing Tools and Methodology in IoT based DF Models

3.1 OSForencics

OSForensics is a live forensics tool which provides various features to extract evidence from various kinds of files including web browser,emails,text,images etc by analyzing in a live system. Its provide an easy and user friendly forensics tool which extract meaningful evidence from the system. It’s also provide features to display recent activity without effecting the system evidences that’s makes it’s a leading live acquisition tools.

3.2 BulkExtractor

Its a forensic tool which used to extract and carve files from compressed files, pdf ,incomplete and partially corrupted files and folders. It’s provides a user interface which for bulk extraction which also provides feature for malware analysis . Its take care of the evidence and intelligence data while extracting the bulk data from the devices. The main features provided by the BulkExtractor are data reduction method and Data Reduction by Selective Imaging for digital forensics analysis. Furthermore, its is useful to extract data from hard drives, IoT devices, optical media, camera cards etc.

3.3 FOREMOST

It provides console which allows to execute the process called data carving by forensic examiners. This process is used to regained partial or full files from a bit image based on their internal data structure and their headers and footers. This process is also known as data carving. Its also provide the option to recover only the selected type files from the system for the further forensics process which makes the investigator flexibility in their process.

3.4 WireShark

Wireshark is a forensics tool started in the year 1998 by Gerald Combs which is initially named as Ethereal later renamed in the year 2006 is an open source widely used network forensics packet analyzer tool with user interface used to analyze the packets in the wired or wireless connectivity of network simplifies to analyze the packets and connectivity in the network which display live or in a file which recorded the flow of packets.It also an important tool which serves the role of identification and gathering information about the protocol information and sniffing packets traversing in between the interconnected IoT devices.[1]

As an efficient tools for network forensic its provides information related to the packet source and destination IP address as well as port information which helps the investigator to leads their investigation further in an correct direction.

3.5 X-Ways

X-Ways is a highly flexible and portable forensic tool by providing features like file carving, disk imaging and cloning ,extraction of lost or deleted data, ensuring data authenticity, Disk cleaning ,file detection , running process acquisition, provides data recovery techniques and many more.

3.6 FTK Imager

FTK imager is a high speed multi threaded distributed processing forensics tool designed for data extraction from the compromised devices. By calculating the MD5 hash value its check the file integrity while extraction .In addition to this it also used for disk imaging and cloning of Hard drive, CDs , USB derives also.

3.7 Autospy

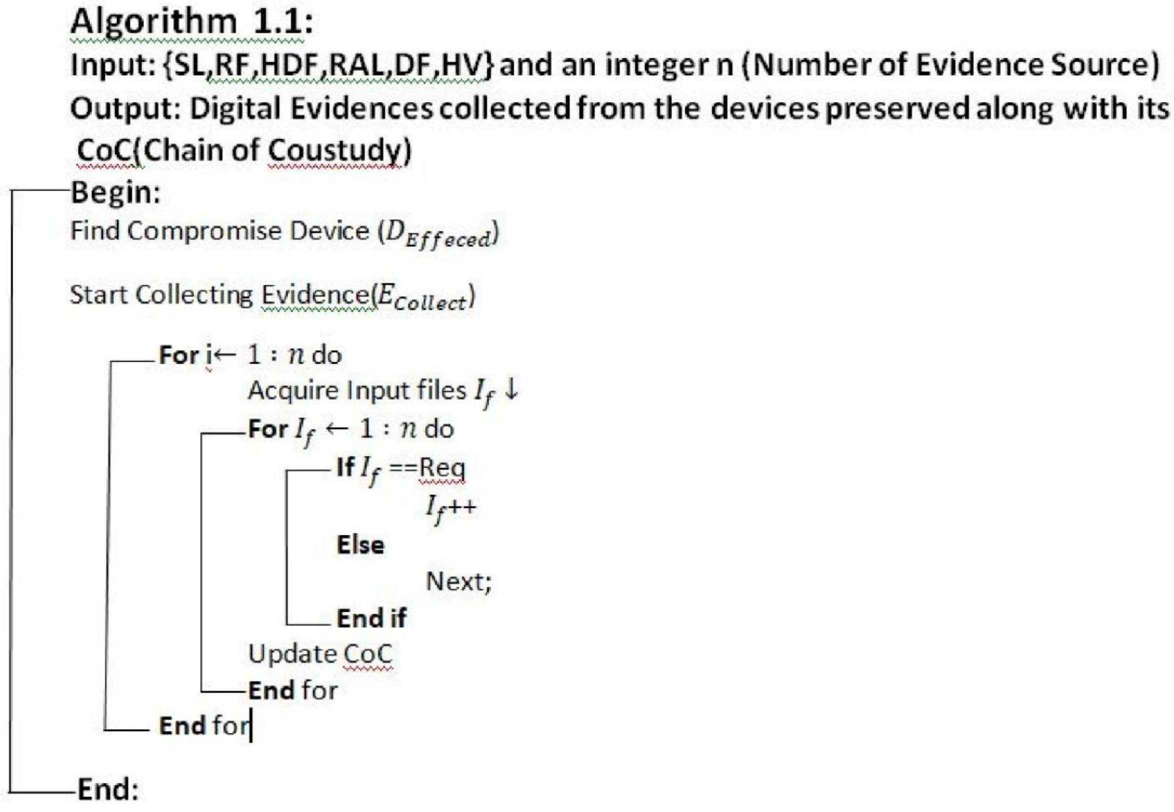
Autospy is an automated evidence analysis tool . by using NIST NSRL, EnCase, Hash Keeper, and MD5 hash database formats analyzing disc images, local drives, and directories to determine possible causes of an event. Its provides a user interface which display all the details of data which helps in investigation . It supports file-system types, such as NFTS, FAT12/16/32, Ext2/3/4, HFS/HFS+, ISO9660, and UFS.Most importantly it provides site artifact analysis and registry Analysis which makes its unique then other forensic tools.[12]

3.8 MemGator

MemGater is an open source, portable, cross platform and server tool provide a CLI written in Go language. Its provide a report by extracting data from the files automatically which is used by the examiner at the time of memory analysis. The report may contain anything like details, password, process, malware detection, network connection, encryption key etc.[12]

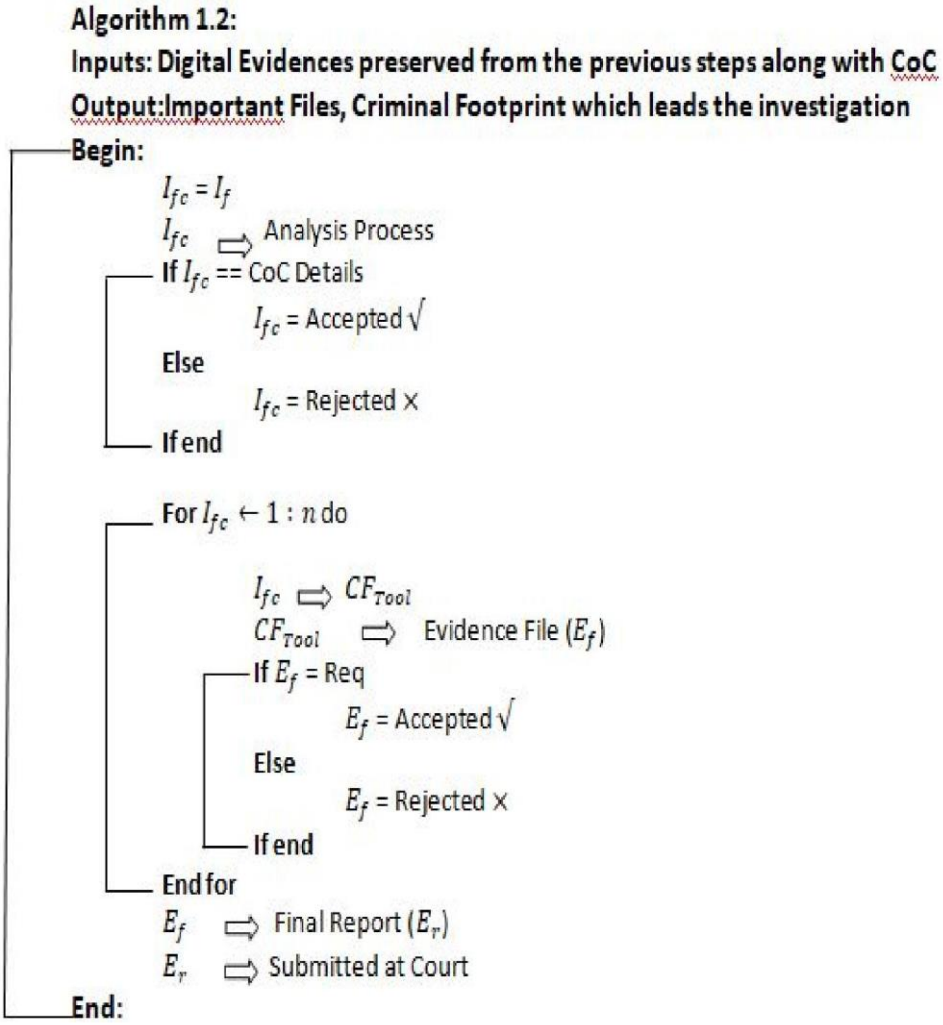
4 State of Art result and Analysis 4.1 Algorithm

After the systematic state of art analysis the overall forensic process with the digital evidences is algorithmically represented in algorithm 1.1 and 1.2 . The algorithms mimic a novel step by step representation of IoT forensic process as per the current industry standard.



```
Algorithm 1.1:
Input: {SL,RF,HDF,RAL,DF,HV} and an integer n (Number of Evidence Source)
Output: Digital Evidences collected from the devices preserved along with its
 CoC(Chain of Coustudy)
Begin:
Find Compromise Device ($D_{Effeced}$)
Start Collecting Evidence($E_{Collect}$)
    For i← 1 : $n$ do
        Acquire Input files $I_f$ ↓
        For $I_f$ ← 1 : $n$ do
            If $I_f$ ==Req
                $I_f$++
            Else
                Next;
            End if
        Update CoC
        End for
    End for
End:
```

Algorithm 1.1 defines the process of Identification, Acquisition and Preservation in the IoT forensics process in an algorithmic way.This phase carried out in the crime location where the investigators collect evidences from the devices available.Here in this phase maintaining the CoC is an important work which ensures the integrity of the evidence .



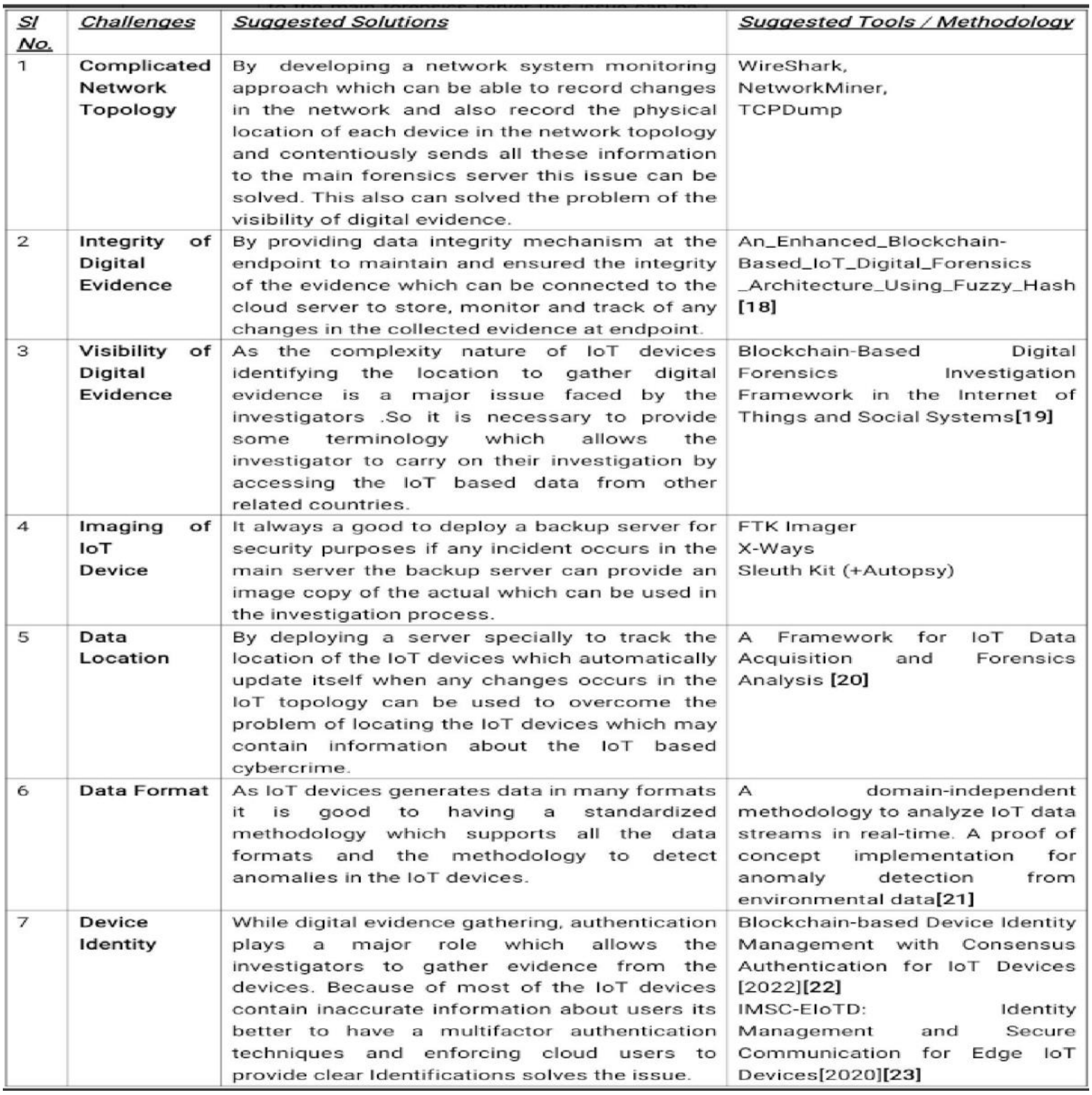
```
Algorithm 1.2:
Inputs: Digital Evidences preserved from the previous steps along with CoC
Output:Important Files, Criminal Footprint which leads the investigation
Begin:
    $I_{fc} = I_f$
    $I_{fc}$ ⇨ Analysis Process
    If $I_{fc}$ == CoC Details
        $I_{fc}$ = Accepted √
    Else
        $I_{fc}$ = Rejected ×
    If end

    For $I_{fc} \leftarrow 1 : n$ do
        $I_{fc}$ ⇨ $CF_{Tool}$
        $CF_{Tool}$ ⇨ Evidence File ($E_f$)
        If $E_f$ = Req
            $E_f$ = Accepted √
        Else
            $E_f$ = Rejected ×
        If end
    End for
    $E_f$ ⇨ Final Report ($E_r$)
    $E_r$ ⇨ Submitted at Court
End:
```

Algorithm 1.2 is the process of analysis and report presentation where the analysis team extract the useful evidences to proof the crime committed by the cyber criminal by examining the evidence collected in the previous phase of investigation.

4.2 Problems and Solution

Table 2:Challenges and Suggestion in IoT Forensics



Sl No.	Challenges	Suggested Solutions	Suggested Tools / Methodology
1	Complicated Network Topology	By developing a network system monitoring approach which can be able to record changes in the network and also record the physical location of each device in the network topology and contentiously sends all these information to the main forensics server this issue can be solved. This also can solved the problem of the visibility of digital evidence.	WireShark, NetworkMiner, TCPDump
2	Integrity of Digital Evidence	By providing data integrity mechanism at the endpoint to maintain and ensured the integrity of the evidence which can be connected to the cloud server to store, monitor and track of any changes in the collected evidence at endpoint.	An_Enhanced_Blockchain-Based_IoT_Digital_Forensics _Architecture_Using_Fuzzy_Hash [18]
3	Visibility of Digital Evidence	As the complexity nature of IoT devices identifying the location to gather digital evidence is a major issue faced by the investigators .So it is necessary to provide some terminology which allows the investigator to carry on their investigation by accessing the IoT based data from other related countries.	Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems[19]
4	Imaging of IoT Device	It always a good to deploy a backup server for security purposes if any incident occurs in the main server the backup server can provide an image copy of the actual which can be used in the investigation process.	FTK Imager X-Ways Sleuth Kit (+Autopsy)
5	Data Location	By deploying a server specially to track the location of the IoT devices which automatically update itself when any changes occurs in the IoT topology can be used to overcome the problem of locating the IoT devices which may contain information about the IoT based cybercrime.	A Framework for IoT Data Acquisition and Forensics Analysis [20]
6	Data Format	As IoT devices generates data in many formats it is good to having a standardized methodology which supports all the data formats and the methodology to detect anomalies in the IoT devices.	A domain-independent methodology to analyze IoT data streams in real-time. A proof of concept implementation for anomaly detection from environmental data[21]
7	Device Identity	While digital evidence gathering, authentication plays a major role which allows the investigators to gather evidence from the devices. Because of most of the IoT devices contain inaccurate information about users its better to have a multifactor authentication techniques and enforcing cloud users to provide clear Identifications solves the issue.	Blockchain-based Device Identity Management with Consensus Authentication for IoT Devices [2022][22] IMSC-EIoTD: Identity Management and Secure Communication for Edge IoT Devices[2020][23]

To overcome the short falls found during the forensics process faced by the forensic investigators is depicted in table 2 as a whole. [18] [19] [20] [21] [22] [23]

5 Conclusion

Due to the constant rise of cyber crime and forensics in IoT environment emerges major challenges to the security researcher's community. This paper reviews all the latest trends of digital forensics tools, equipments in IoT enabled digital forensic environment following the recent state of art literatures . Step by step forensics process is depicted with the high end tools to meet the cyber secured approach. A novel algorithmic approach of IoT forensic process is suggested to mitigate the emerging challenges . This paper can be extended towards IoMT and IoVT based forensics environments to deal with the cyber crime using ML.

References

[1] Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., Markakis, E.K.: A survey on the internet of things (iot) forensics: challenges, approaches, and open issues. IEEE Communications Surveys & Tutorials 22(2), 1191–1221 (2020)

[2] Sachdeva, S., Raina, B., Sharma, A.: Analysis of digital forensic tools. Journal of Computational and Theoretical Nanoscience 17(6), 2459–2467 (2020)

[3] Alghamdi, M.I.: Digital forensics in cyber security—recent trends, threats, and opportunities. Cybersecurity Threats with New Perspectives (2021)

[4] Majed, H., Noura, H.N., Chehab, A.: Overview of digital forensics and anti-forensics techniques. In: 2020 8th International Symposium on Digital Forensics and Security (ISDFS), pp. 1–5 (2020). IEEE

[5] Quick, D., Choo, K.-K.R.: Iot device forensics and data reduction. IEEE Access 6, 47566–47574 (2018)

[6] Kohnehshahri, K.D., Kargar, M.H., Soleimani-Roozbahani, F.: The effect of using coap protocol on reducing energy consumption in smart houses (case study: Uromieh culture house). International Journal of Advanced Networking and Applications 10(3), 3843–3852 (2018)

[7] Quick, D., Choo, K.-K.R.: Impacts of increasing volume of digital forensic data: A survey and future research challenges. Digital Investigation 11(4), 273–294 (2014)

[8] McKemmish, R.: When Is Digital Evidence Forensically Sound? Springer, ??? (2008)

[9] Cosic, J., Cosic, Z.: Chain of custody and life cycle of digital evidence. Computer technology and application 3(2) (2012)

[10] Alex, M.E., Kishore, R.: Forensics framework for cloud computing. Computers & Electrical Engineering 60, 193205 (2017)

[11] O’shaughnessy, S., Keane, A.: Impact of cloud computing on digital forensic investigations. In: Advances in Digital Forensics IX: 9th IFIP WG 11.9 International Conference on Digital Forensics, Orlando, FL, USA, January 28-30, 2013, Revised Selected Papers 9, pp. 291–303 (2013). Springer

[11] Alazab, A., Khraisat, A., Singh, S.: A review on the internet of things (iot) forensics: Challenges, techniques, and evaluation of digital forensic tools (2023)

[12] Rana, N., Sansanwal, G., Khatter, K., Singh, S.: Taxonomy of digital forensics: Investigation tools and challenges. arXiv preprint arXiv:1709.06529 (2017)

[13] Atlam, H.F., Hemdan, E.E.-D., Alenezi, A., Alassafi, M.O., Wills, G.B.: Internet of things forensics: A review. Internet of Things 11, 100220 (2020)

[14] Casino, F., Dasaklis, T.K., Spathoulas, G.P., Anagnostopoulos, M., Ghosal, A., Borocz, I., Solanas, A., Conti, M., Patsakis, C.: Research trends, challenges, and emerging topics in digital forensics: A review of reviews. IEEE Access 10, 25464– 25493 (2022)

[15] Meffert, C., Clark, D., Baggili, I., Breitinger, F.: Forensic state acquisition from internet of things (fsaiot) a general framework and practical approach for iot forensics through iot device state acquisition. In: Proceedings of the 12th International Conference on Availability, Reliability and Security, pp. 1–11 (2017)

[16] Janarthanan, T., Bagheri, M., Zargari, S.: Iot forensics: an overview of the current issues and challenges. Digital Forensic Investigation of Internet of Things (IoT) Devices, 223–254 (2021)

[17] Mahrous, W.A., Farouk, M., Darwish, S.M.: An enhanced blockchain-based iot digital forensics architecture using fuzzy hash. IEEE Access 9, 151327–151336 (2021)

[18] Li, S., Qin, T., Min, G.: Blockchain-based digital forensics investigation framework in the internet of things and social systems. IEEE Transactions on Computational Social Systems 6(6), 1433–1441 (2019)

[19] Chi, H., Aderibigbe, T., Granville, B.C.: A framework for iot data acquisition and forensics analysis. In: 2018 IEEE International Conference on Big Data (Big Data), pp. 5142–5146 (2018). IEEE

[20] Trilles, S., Belmonte, `O., Schade, S., Huerta, J.: A domain-independent methodology to analyze iot data streams in real-time. a proof of concept implementation for anomaly detection from environmental data. International Journal of Digital Earth 10(1), 103–120 (2017)

[21] Mukhandi, M., Damião, F., Granjal, J., Vilela, J.P.: Blockchain-based device identity management with consensus authentication for iot devices. In: 2022 IEEE

[22] 19th Annual Consumer Communications & Networking Conference (CCNC), pp. 433–436 (2022). IEEE

[23] adique, K.M., Rahmani, R., Johannesson, P.: Imsc-eiotd: identity management and secure communication for edge iot devices. Sensors 20(22), 6546 (2020)