Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

A Study on Iot Forensic Investigation in the New Age of Intelligent Crimes

G.Rekha [#1], Dr.T.Sudha [*2]

[1.]Research scholar,Department of CSE, SOET,Sri Padmavati Mahila Visvavidyalayam,Tirupati, AP,India.

E-mail: rekha.spmvv@gmail.com

[2.] Professor,Department of Computer Science,Sri Padmavati Mahila Visvavidyalayam,Tirupati, AP,India.

E-mail: thatimakula_sudha@yahoo.com

Article Info
Page Number: 3274-3281
Publication Issue:
Vol. 71 No. 4 (2022)

Article History
Article Received: 25 March 2022
Revised: 30 April 2022
Accepted: 15 June 2022
Publication: 19 August 2022

Abstract
The deployment of IoT devices is increasing quickly across many industries, notably in the medical service sector. The amount of information produced by connected devices is massive, and it may be in a multitude of various forms. There is also no assurance that the information and devices are safe. If the hardware fails as a consequence of these assaults, it may risk personal lives assuming a direct link exists. As a result, if significant IoT-related cybercrime is identified, a lengthy inquiry is necessary. This includes obtaining sufficient evidence through such IoT units in order to conduct a complete investigation, and the gathered evidential data must be preserved. The major goal of this research is to offer a comprehensive picture of the potential concerns associated with IoT forensic challenges and how Blockchain technology could be incorporated to safeguard potential evidence information acquired from an IoT cybercrime environment.

Keywords: - Blockchain, Distributed Digital Ledger Technology, IoT Forensics,Digital Forensics,Digital shreds of Evidences.

1.Introduction

With the expansion of the internet, it is observed that the expansion of unlawful acts and digital crime necessitates a distinct and original type of forensics knowledge. If anybody exploits your online activity to steal your money or, worse, your identity, professionals require digital forensics to look for digital footprints in order to find the guilty party.IoT, on the other hand, presents a new degree of cyber-threat. Your online activity is no longer limited to either desktop or smartphone gadgets; nowadays it encompasses home automation, linked automobiles, and a variety of other gadgets.Apparently, the smart pet collars allow malicious actors to obtain your info.IoT forensics seeks to mimic the process of any forensics practice, with investigators identifying, interpreting, preserving, analyzing, and presenting any pertinent data.

However, gathering this information can indeed be difficult since it is typically stored on the supplier's cloud platform rather than within the devices themselves. If you are able to extract the data from the device, you will need to use one of several approaches due to the different structures of IoT devices' equipment, application, and firmware. So, while solid and informative information is accessible, obtaining it is a significant job.The function of IoT in the environment of crime should also be considered by regulators. Was indeed the IoT gadget used to conduct the crime, or was it purely a bystander? Police recovered an Amazon Echo device from the residence in which the murder occurred in Bentonville, Arkansas, in 2015. Since Echo devices may occasionally start picking up and recording incomplete conversations (as well as explicit orders), authorities obtained a warrant to Amazon for just about any data acquired by the device. Likewise, in the case of a 2017 double homicide in Farmington, New Hampshire, a court issued a summons requiring Amazon to provide two days' worth of audio recordings from an Amazon Echo, in the belief that it captured some of the assault. In both cases, Amazon was noticeably hesitant and/or delayed to react to investigators' requests for consumer information.While people understand that IoT devices capture, retain, and exchange vital information to help us make personal and commercial decisions, we can observe ever-changing uses even during these early phases of linked devices. The potential for such assets to incite new crimes generates a whole new level of apprehension in the public, but their capacity to capture and store data might be useful for detectives without other leads. Leading technology firms must also resolve how they decide to assist (or not assist) police considering that their own gadgets may hold the key to solving potentially violent criminal proceedings.

Furthermore, there is no assurance that the confidential personal information and devices will be secure. If the technology fails as a consequence of one of the assaults, If there is a direct correlation, it may endanger human life.. Comprehensive investigations are essential if potential IoT-related fraud is discovered. To undertake a thorough inquiry, enough evidence from various IoT contexts is required. After acquiring the evidence, it must be properly kept; otherwise, the additional inspection may result in an incorrect finding. If false information is used as a basis for the investigation, it may result in incorrect conclusions. As a result, the inappropriate individual or group may be accused of the assault, perhaps leading to legal complications. Following are some details on how IoT, IoT Forensics(IoTF), Digital Forensics (DF), and IoT Safety differ from one another.

1.1. IoT Vs IoTF

IoT is a collection of tangible items that are sensor- and actuator-equipped that communicate with one another or with cloud servers without the need for human or computer intervention. Things were usually general names for the items. A subcategory of digital forensics is IoT forensics. which utilizes digital pieces of evidence as inputs to conduct various investigative techniques once a cyber-related criminal activity happens.

1.2. IoTF Vs DF

IoTF is a branch of DF that aims to locate, gather, and investigate digital evidence. The basic distinction is that the sources of pieces of evidentiary information are increasingly fragile in IoT situations. For example, the evidential information collected from traffic signals, moving autos, smart gadgets, and so on and so forth. However, there aren't many sources available in DF for bits of proof. Computers, laptops, cellphones, and various entry points may be used to collect it. On the other hand, It is increasingly challenging to collect evidence from varied IoT contexts.

1.3. IoTF Vs IoT Security

IoTF investigation is a specific instance that indicates they would only use such forensic investigation techniques whenever A cyber-crime involving IoT occurs.. To put it simply, IoT security is a general phrase that implies that must and should offer the essential defensive lines against various assaults 24 hours daily.

2. Literature Survey

The researchers V. R. Kebande et al.'s [1] [2] Digital Forensics Investigation Framework conforms with ISO/IEC 27043: 2015, a well-known guideline for incident investigation principles. The authors' techniques offer the benefit of getting easily transferable to many IoT scenarios. However, They lack fundamental information. that would enable them to respond to various scenarios without changing any crucial elements or methods.

The investigation conducted by the researchers Xiaohua et al.[3] demonstrates how the Raspberry Pi devices could be readily penetrated due to improper (default) setup. The experts recommend reviewing the equipment's parameters to guarantee that it is running in a forensically sound manner. Additionally, it has been shown that the device's digital forensics investigation may access data that is probably evidence.

The FSAIoT platform developed by D. Clark et al.[4] consists of a centralized Forensic State Acquisition Controller model (FSAC) that gathers information in several ways: controller to IoT device, controller to cloud, and controller to controller.

IoT conceptual model by A. Varol et al. [5] presents forensic and evidence gathering problems.

The device constituting the final node in the communications network must be reviewed first, based on the authors' LoS Algorithm. The evidence recognition procedure, according to the NBT paradigm, begins at device level and proceeds across succeeding zones.

R. Rios et al. [7] introduced the PRoFIT paradigm, This incorporates the ISO/IEC 29100:2011 guideline all across the forensic testing process even while considering safety into account.This suggested design emphasizes the significance of communicating with nearby gadgets that gather data and replicate crime scene In fact, the suggested method has been altered to incorporate the concept of a digital witnesses.

The study has reviewed [8,] EM-SCA approaches Such issues have been resolved when partnered with machine learning methods...[9] analyzes the usefulness of a Hyperledger Composer-based Forensic Network architecture design. Using the improved end-to-end application, the researchers demonstrated satisfactory performance and resource usage overhead. However, this analysis does not include a totally ideal unified framework to preserve evidential information, which is underpin mostly by the IPFS and HyperLedger fabric. Further this research might be improved by including a Blockchain which tracks each forensic investigator's activities.

S. Singh et al.[10] presents a smart home architecture that is simultaneously economical and secure, based on cloud processing and ledger technologies. To assure privacy and security in a localized smart home automation web, the authors utilized cryptographic plus a hashed method in Ethereum technology. For identifying the link among traffic parameters, the MCA (Multivariate Correlational Analysis) detection approach is used.

E. Pilli et al. [11] developed a complete IoTF framework built on the ISO/IEC 27043 global standard. The architecture is divided into three major phases: forensic preparation, forensic initiation , and forensic investigation.

A. K. Sikder et al. [12] advocated the use of IoTDots to proactively analyze and change smart apps to locate and store forensically sound information. It is made up of two key parts: the Modifier (ITM) and the Analyzer. Whenever ITM detects relevant data, it transfers it to a protected database. In a later step, IoTDots employs machine learning to extract relevant information from IoT devices, apps, or user actions. The creators, however, failed to take security precautions into consideration when changing the device's firmware.

The approach followed in [13],[14] leverages a loosely coupled design by combining a blockchain component alongside a current memory module to provide proof of consistency and authenticity checks. The blockchain module makes use of a hybrid blockchain architecture and a PBFT (Practical Byzantine fault tolerance) method that has been optimized. To provide confidentiality and traceability, multi-signature techniques based on randomized and certificated key pairs are utilized.

WAEL A et al.[15] authors applied the Fuzzy Hash approach for detecting similarities between digital fingerprints of digital evidence, and then they used a blockchain distributed ledger to secure the digital evidence gathered from IoT-related cybercrime.However, fuzzy hashing falls short when it comes to detecting patterns in binary packets, and it is an area where more study and development are needed.A further difficulty with fuzzy hashing is that there's still presently no mechanism to dynamically evaluate whether a result is favorable or unfavorable, hence the only safe technique would be to do it explicitly.

FARHAN ULLAH et al.[16] suggested a deep learning-based solution for identifying pirated and malicious files.The trial findings suggest that the integrated strategy surpasses cutting-edge approaches in terms of categorizing outcomes. The tokenization method pulls keywords from source codes yet does not display the inner view of source codes. However this experiment does not concentrate on pirated copies and unknown malware families.

Rizky Tri Wiyono et al.[17] suggested Decision Tree C4.5 as a Classifier Method for Botnet Activities in the IoT. This work is mainly focused on network level bot IoT performance analysis and it is not meant for device level and cloud level analysis.

Honghe Zhou et al.[18] has developed a method for doing IoT forensics on autonomous robot vacuum devices and conducted a forensic application-level investigation of the iRobot smart vacuum and its app. They have proved the capability of extracting confidential data such as use patterns, the clear routine of the user, user identification number and network information, and so on, through thorough trials.The pilot research in this report is limited at the application level.

George Grispos et al.[19] presented a IoT ecosystem to assess the capacity to retrieve client and gadget details via another devices' flash memory The findings of this study may also be utilized to determine if gadget production should incorporate forensic-by-design concepts in order to improve forensics examinations for IoT devices.

3. Evidence Acquisition Levels

The existing conventional forensics investigation procedures use mainly three levels to collect shreds of evidence.

- Media /Device level
- Network level
- Cloud level

The facts can be obtained via all three levels listed below.

3.1. Device/Media level data Acquisition: Investigators can employ the JTag and Chip off processes to recover the device's internal flash memory, however this might be a headache for forensic investigators because flash memory segments cannot be removed sequentially, but rather are dispersed across the whole memory. What if the gadget is implanted in an individual? How might the obvious data be always recovered? This is an extremely challenging issue to solve.

3.2. Network log information Acquisition: Network records are an apparent type of data, but mostly because IoT links are radical, networking records may be rapidly updated.

3.3. Cloud data Acquisition: Vast amount of information from IoT devices is saved on cloud systems, and while cloud records may indeed be taken into account as a part of the apparent data, Content stored on cloud platforms is not immune to numerous assaults.; in reality, mostly sensitive to attacks.

4. Proposed System Architecture

The existing conventional forensic models do not have any unified design to capture then evidential information at all levels. So ,the creation of an unique Blockchain network to preserve evidence acquired from such an IoT-related Cyber-crime incident and also to assure high availability and evidence integrity. If we integrate IoT with one of the Blockchain techniques called public digital ledger we can achieve high availability of evidence and we can ensure integrity, confidentiality, and non-repudiation.

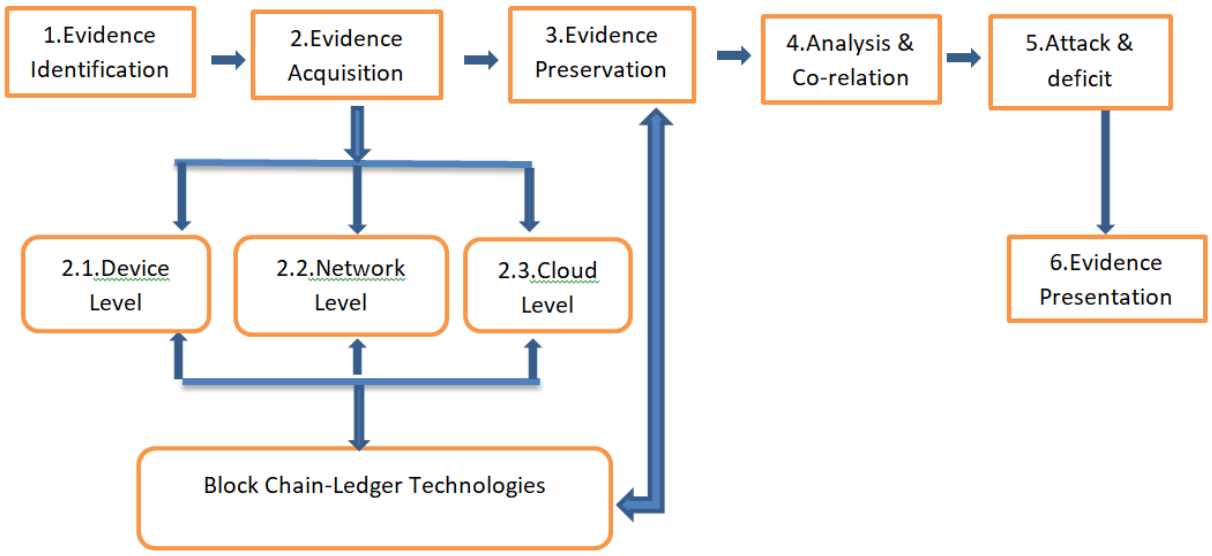

Fig .1: Proposed System Architecture

Figure 1 depicts the stages of IoT Forensic investigations that include the use of Blockchain ledger technology to safeguard evidence obtained from the IoT cyber crime scenario.

5. Conclusion

When blockchain ledger technologies are employed to keep evidence of an IoT-related cyber-crime, the evidence is securely stored and kept, and a single point of failure is eliminated. This ensures the high availability, integrity, and confidentiality of the information. Because of the blockchain network contains extremely secure hash algorithms, it is relatively straightforward to safeguard metadata connected to evidence stored on the blockchain.

References

1. V. R. Kebande and I. Ray, “A generic digital forensic investigation framework for Internet of Things (IoT),” in Proc. IEEE 4th Int. Conf. Future Internet Things Cloud (FiCloud),2016
2. V. R. Kebande and H. S. Venter, “Novel digital forensic readiness technique in the cloud environment,” Aust. J. Forensics Sci., vol. 50, no. 5, pp. 552–591, 2018

3. Xiaohua, FengOnafeso, BabatundeEnjie Liu,"Cyber security investigation for Raspberry Pi devices" 10547/622090 ,University of Bedfordshire Repository, June,2017.
4. C. Meffert, D. Clark, I. M. Baggili, and F. Breitinger, "Forensic state acquisition from Internet of Things (FSAIoT)," in Proc. 12th Int. Conf.Availability Rel. Security (ARES), 2017.
5. M. Harbawi and A. Varol, "An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework," in Proc. 5th Int. Symp. Digit. Forensics Security (ISDFS), 2017
6. T. A. Zia, P. Liu, and W. Han, "Application-specific digital forensics investigative model in Internet of Things (IoT)," in Proc. 12th Int. Conf. Availability Rel. Security (ARES), 2017.
7. A.Nieto, R. Rios, and J. Lopez, "IoT-forensics meets privacy: Towards cooperative digital investigations," Sensors, vol. 18, no. 2, p. E492, Feb. 2018
8. Asanka Sayakkara,Nhien-An Le-Khac,Mark Scanlon "Leveraging Electromagnetic Side-Channel Analysis for the Investigation of IoT Devices", DFRWS USA,April,2019.
9. Auqib Hamid Lone, RoohieNaaz Mir,"Forensic-chain: Blockchain based digital f orensics chain of custody with PoC in Hyperledger Composer",January pp. 44-55,2019,Digital Investigation, Elsevier.
10. S. Singh, I. H. Ra, W. Meng, M. Kaur, and G. H. Cho, "SH-BlockCC: A secure and efficient Internet of Things smart home architecture based on cloud computing and blockchain technology," Int. J. Distrib. Sens. Netw., vol. 15, no. 4, pp. 1–18, March 2019.
11. L. Sadineni, E. Pilli, and R. B. Battula, A Holistic Forensic Model for the Internet of Things. Cham, Switzerland: Springer Int., IFIPAICT, volume 569, pp. 3–18, August 2019.
12. L. Babun, A. K. Sikder, A. Acar, and A. S. Uluagac, "A digital forensics framework for smart settings," in Proc. WiSec, May 2019.
13. Z. Tian, M. Li, M. Qiu, Y. Sun, and S. Su, "Block-DEF: A secure digital evidence framework using blockchain," Inf. Sci., vol. 491, pp. 151–165, April. 2019.
14. H. Abie, "Cognitive cybersecurity for CPS-IoT enabled healthcare ecosystems," in Proc. Int. Symp. Med. Inf. Commun. Technol. (ISMICT), May 2019.
15. Wael A. Mahrous, Mahmoud Farouk, And Saad M. Darwish "An Enhanced Blockchain-Based IoT Digital Forensics Architecture Using Fuzzy Hash", IEEE ACCESS, VOLUME 9, 2021.Digital Object Identifier 10.1109/ACCESS.2021.3126715.
16. Farhan Ullah , Hamad Naeem , Sohail Jabbar , Shehzad Khalid , Muhammad Ahsan Latif , Fadi Al-Turjman," Cyber Security Threats Detection in the Internet of Things Using Deep Learning App roach ",SPECIAL SECTION ON DATA MINING FOR INTERNET OF THINGS,IEEE ACCESS,September 13, 2019.
17. Rizky Tri Wiyono, Niken Dwi Wahyu Cahyani "Performance Analysis of Decision Tree C4.5 as a Classification Technique to Conduct Network Forensics for Botnet Activities in the Internet of Things", International Conference on Data Science and Its Applications (ICoDSA),2020.

18. Honghe Zhou, Lin Deng, Weifeng Xu, Wei Yu , osh Dehlinger , and Suranjan Chakraborty “Towards Internet of Things (IoT) Forensics Analysis on Intelligent Robot Vacuum Systems ”,2022 IEEE/ACIS 20th International Conference on Software Engineering Research, Management and Applications (SERA), IEEE,2022, DOI: 10.1109/SERA54885.2022.9806735.
19. George Grispos, Frank Tursi, Kim-Kwang Raymond Choo†, William Mahoney and William Bradley Glisson,” A Digital Forensics Investigation of a Smart Scale IoT Ecosystem”, IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom),2021.