Multimedia Tools and Applications (2021) 80:36183–36214
https://doi.org/10.1007/s11042-021-11350-9

A review study on blockchain-based IoT security and forensics

Randa Kamal[1] · Ezz El-Din Hemdan[1] · Nawal El-Fishway[1]

Received: 14 October 2020 / Revised: 10 July 2021 / Accepted: 26 July 2021 /
Published online: 1 September 2021

Abstract

The term Internet of Things (IoT) represents all communicating countless heterogeneous devices to share data and resources via the internet. The speedy advance of IoT devices proposes limitless benefits, but it also brings new challenges regarding security and forensics. Likewise, IoT devices can generate a massive amount of data that desires integrity and security during its handling and processing in an efficient way. IoT devices and data can be vulnerable to various types of cyber-crimes at each IoT layer. For combating these cyber-crimes in IoT infrastructure, IoT forensic term has shown up. The IoT forensic is the process of performing digital forensic investigation in the IoT environment in a forensically sound and timely fashion manner. Sundry challenges face the IoT forensics that requires urgent solutions and mitigation methods; digital evidence needs to be collected, preserved, analyzed, processed, and reported in a trusted manner to be acceptable for presenting in the court of law. Preserving the evidence unchanged or tampered with is the most critical challenge in digital forensics. Authentication is another challenge facing digital forensics; who is allowed to deal with the evidence? One of the most recent solutions for supporting IoT forensics is the use of Blockchain. Using Blockchain in digital forensics guarantees data integrity, immutability, scalability, and security. Therefore, this paper presents a comprehensive review of IoT security and forensics with the integration with Blockchain technology. It begins by providing an inclusive discussion of IoT security, as well as the need for IoT forensics, and the concepts of Blockchain. Then, a review of Blockchain-based IoT security and forensics issues is presented. Finally, a discussion of open research directions is provided.

Keywords Cybercrimes · Digital forensics · IoT security · Blockchain · IoT forensics

✉ Randa Kamal
randa.soltan@te.eg

Ezz El-Din Hemdan
ezzvip@yahoo.com

Nawal El-Fishway
nelfishawy@hotmail.com

[1] Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menoufia, Egypt

1 Introduction

Recently, there is no doubt that the Internet of Things (IoT) is the next generation of communicating various types of sensor/actuator-embedded devices over the internet [18]. These devices are of different types; from tiny wearable devices with microcontroller units [67] to huge instrumental devices or smart grids [8, 61]. The benefits of using IoT are well known like facilitating the communication between people around the world, taking appropriate decisions in critical situations based on sensed data from the surrounding environment, or even preventing some crimes or disasters from happening. [127]. These benefits do not come without a cost; IoT networks and devices are vulnerable to many threats for hardware, software, network, or applications or even the services may become inoperable due to poor Internet connections [127].

Numerous threats were analyzed and many solutions have been introduced for solving the security problems. These solutions are categorized into four main categories according to the used technology. These categories are fog computing, edge computing, machine learning, and Blockchain-based solutions [42]. One notable solution for cyber-attacks in IoT was using Blockchain which successfully has solved many kinds of these attacks but it still has its drawbacks. In this paper, we introduce an overview of IoT and its threats, cybersecurity, and how it differs from regular IT security and how can Blockchain solve these problems, and some of the future work to improve it.

On the other hand, IoT Digital forensics is a very significant topic that needs special tools for analyzing the huge amount of data from the crime scene. It can be defined as the process of extracting, analyzing digital evidence from a crime scene to reconstruct the crime in IoT infrastructure [49]. Today, there are very complex challenges of IoT Digital forensics investigation than traditional forensics. One of them is the lack of the appropriate forensics tools which can support various types and models of IoT devices in the market while the other is the un-clarity of the network boundaries between connected devices [49]. These new challenges need modern models for analyzing the massive amount of digital evidence. Digital evidence is defined according to [81] as "*the information stored or transmitted in binary form that may be relied on in court*". The sources of digital evidence may be in the form of text messages, images, call logs of cell phones, network access logs, internet browser history of computers of laptops, chat sessions, passwords, documents, spreadsheets, and databases. This paper introduces a review study on the use of Blockchain in Securing the IoT forensics processes and assisting digital investigators in performing cybercrimes investigation in IoT infrastructure in a forensically sound manner. Therefore, the contribution of this paper can be summarized as the following:

- Exploring concepts and applications of IoT with its security issues.
- Investigating challenges, requirements, and opportunities of IoT forensics.
- Highlighting the state-of-the-art research and recent studies of digital forensics in IoT infrastructure.
- Presenting perceptions and concerns of Blockchain for both digital forensics and IoT Security.
- Discussing open research directions of this innovative paper's subject.

The structure of the rest of this paper is organized as follows Sect. 2, provides an overview of the Internet of Things definition, applications, layers, advantages and challenges, and cyber-attacks while the concept of IoT forensics is provided in Sect. 3. Section 4 presents the characteristics, challenges of Blockchain for IoT security while the challenges and opportunities of applying Blockchain to IoT forensics are presented in Sect. 5. Finally, the conclusion and open research points in this innovative theme are presented in Sect. 6.

2 IoT security

Internet of Things (IoT) refers to a heterogeneous environment with multiple heterogeneous interconnected devices (i.e. webcams, baby monitors, printers, digital video recorders, Radio Frequency Identification "RFID" and wireless sensors) [58, 92, 96]. The applications of IoT vary from personal applications i.e. health care to huge instrumental applications i.e. smart grids to measure the consumption/production of electrical energy, smart cities, and other applications [82].

The interconnected devices are embedded by both software and hardware to facilitate the performance of the network. Hardware components of the devices include sensors, actuators, and communicating cards. Software components are communicating protocols like TCP/IP and operating systems to manage sensing and transmitting data. The sensed data is transmitted over the internet and stored on a centralized server or the cloud seamlessly [1, 12, 93].

In 2005, the International Telecommunication Union (ITU) defined the internet of things; IoT as "*a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies*" [12].

There are 4 basic elements of IoT systems are physical devices, interconnectivity tools, operating platforms, and real-time applications [38]. The Gartner report announced that there will be around 20.4 billion IoT devices by 2022. From the point of the IoT industry, the revenue is expected to grow from $892 billion in 2018 to $4 trillion by 2025 [42].

2.1 IoT layers

Through the years there were many aspects of the literature concerning categorizing IoT layers [12, 38, 42, 96]. Figure 1 shows the different architectures of IoT. The three basic layers of IoT are:

1. **Sensing or actuating /perception layer:** it is the layer that contains physical IoT devices that sense and respond to different phenomena in the surrounding environment.
2. **Transport/network layer:** this layer gives the ability to the data to be transferred between the devices.
3. **Application layer:** this layer is responsible for the storage, analysis, and representation of the sensed data to the end-user.

While the four layers in IoT are:

1. **sensors and actuators:** they are the physical sensors "to sense the surrounding environmental phenomena", and actuators" that perform predefined actions according to the sensed data" for example ultrasonic sensors, temperature and humidity sensors, electrical sensors, etc.

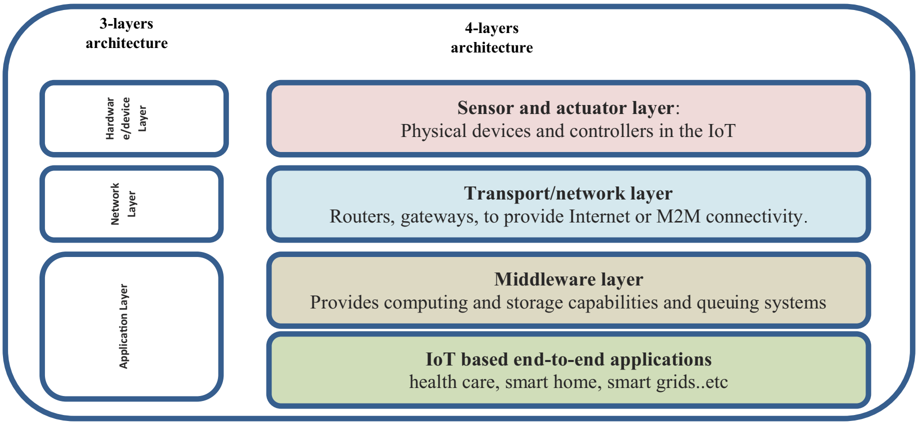

3-layers architecture
4-layers architecture
Hardwar e/device Layer
Network Layer
Application Layer
Sensor and actuator layer: Physical devices and controllers in the IoT
Transport/network layer Routers, gateways, to provide Internet or M2M connectivity.
Middleware layer Provides computing and storage capabilities and queuing systems
IoT based end-to-end applications health care, smart home, smart grids..etc

Fig. 1 The architecture of IoT

2. **Communication network:** to transmit the received information from the previous layer to be processed later.
3. **Middleware layer:** it is an intermediate layer between the communication and application layers. It provides computing and storage resources and queuing systems etc.
4. **IoT-based end-to-end applications:** represents the different applications of IoT; health care, smart home… etc.

The International Telecommunication Union (ITU) architecture of centralized "server/client model" IoT:

1. **Application layer:** such as healthcare, unmanned vehicles, smart grids and ...etc.
2. **Service support and application layer**.
3. **Network Layer:** This includes connecting devices such as routers, gateways, to provide Internet or M2M connectivity.
4. **Device layer:** physical devices and controllers in the IoT.

Authors in [96] suggested new 6 layers architecture of IoT: Physical sensor objects, Local communication, Gateway objects, Internet Communication, Cloud storage, and data analysis, and finally IoT application layers.

While [38] suggested detailed IoT layers with sub-layers;

1. Network management:
2. Perception layer: This represents the bottom layer of the IoT architecture including perception nodes and perception networks. It includes the technologies used for sensing, identification, communication, and actuation with minimum human interaction
3. Transmission layer: It is responsible for transmitting gathered data to the information processing unit using wired or wireless communication via a transmission access network, core network, and local & Wide Area Network.
4. Application layer: It is the topmost layer of the IoT architecture. Its purpose is to provide access to personalized services to the end-users over the network.

2.2 IoT applications

There are many applications based on IoT that can be in several fields such as Personal health care [2, 5, 10, 13, 17, 23, 34, 141], smart homes [6, 54, 70, 85, 138, 139, 144], smart cars, unmanned vehicles and parking systems [21, 30, 32, 40, 62, 71, 106], military [11, 22, 25, 76, 86–88, 146], smart cities [15, 36, 69, 89, 105], transportation, agriculture, smart grids [28, 33, 37, 55, 118, 121], automation networks [27, 72], and Cyber-Physical Systems (CPS) [46, 91, 125]. The mentioned applications can improve the quality of human life to a better level. Some other applications are mentioned in [31].

2.3 Cyber-security in IoT

The security of an IoT object is defined generally as the process of protecting that object against hardware and software threats. Hardware threats include physical damage, loss, or robbery. Software threats include unauthorized access, personal data misuse, hacking the system, or inject malicious code to remotely control the device. The cyber-security system must ensure the integrity and confidentiality of information, while at the same time this information is available whenever needed [1]. There are many domains of security for the surrounding digital world. For many years there was confusion between cyber-security and information security the difference between them is shown in Table 1.

Recently, cyber-security was categorized as a component of information security. It is defined as “protecting information assets by addressing the threats to information processed, stored and transported by internetworked information systems.” [120]. Figure 2 shows the three different domains of security and the relationship among them [120].

In IoT, interconnected devices are vulnerable to cyber-attackers. Most IoT devices have limited storage and energy resources. Both IoT devices and services need to be protected against multiple sources of threats and attacks that target hardware resources, information, and data..etc. [1]. IoT security differs from IT security in many aspects: IT devices are resource-rich, can use complex security algorithms to achieve wide security but lower capabilities, and depend on homogeneous technologies. On the contrary, IoT devices are limited in their hardware and software resources; thus it has to apply lightweight security algorithms, and have many heterogeneous devices and data [42].

Table 1 Difference between cyber-security and information security

Cyber Security	Information Security
It is the method of way to defend the information from outside the resource on the net	It is the method of the way to maintain the information’s confidentiality, integrity, and handiness by protecting data from being changed, removed, or accessed by unauthorized parties
Protects networks against cyber-attacks	Protects information from any threats
Deals with cyberspace dangers	Deals with data protection
Cyber crimes, cyber frauds, and law enforcement	Unauthorized access, disclosure modification, and disruption
Professionals deals with the advanced persistent threat	Professionals prioritize resources before threats
Threats that may or may not exist	It deals with integrity, confidentiality, and availability

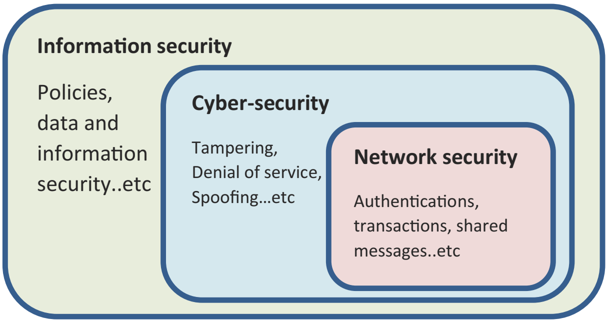

Information security
Policies, data and information security..etc
Cyber-security
Tampering, Denial of service, Spoofing...etc
Network security
Authentications, transactions, shared messages..etc

Fig. 2 The relationship between cybersecurity and other security domains [120]

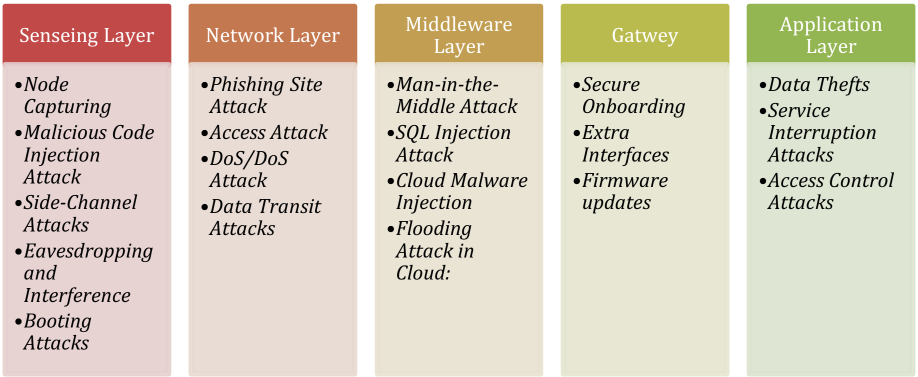
2.4 Types of security attacks

Four major categorized factors that affect the safety of IoT elements [1] are Vulnerabilities, Exposure, Threats, and Attacks as the following:

1. **Vulnerabilities:** They are weaknesses in the system “software, hardware or even users of the system” that allow an attacker to gain unauthorized access to the device and execute commands, steal confidential data, or conduct denial-of-service attacks. Software vulnerabilities are easier to discover and handle than hardware vulnerabilities [48, 51, 68, 79, 95, 108, 136].
2. **Exposure:** It is the problem in the configurations of the devices that allows an intruder to collect personal information. Physical exposures are most challenging, where intruders capture the device itself and modify the programming or even replace it with another malicious device [4, 19, 114, 122, 132, 140].
3. **Threats:** They are some kind of actions based on the system security weakness of the device. Whether these threats are natural “due to environmental factors i.e. flows, fires.. etc.,”or human”internal by authorized individuals or external from outside the network, structured or unstructured”. Good plans should be carefully designed to deal with various types of threats especially natural ones as we cannot prevent them from happening in most cases [7, 41, 42, 73, 101, 137].
4. **Attacks:** They are the actions taken using various techniques and tools by the attackers; where their purpose is to harm a system or disrupt normal operations by exploiting vulnerabilities. Attackers whether they are active or passive can harm the network. The most common attacks are: (a) physical attacks “hardware” [47, 52, 63, 78, 102], (b) Reconnaissance attacks “scanning network ports, or querying IP addresses…etc.,”, (c) Denial-of-service (DoS) [83, 90, 98, 111, 116], (d) Access attacks (physical or remote access” [24, 133, 145], (e) Destructive attacks, Supervisory Control and Data Acquisition (SCADA) Attacks. Attacks on privacy Track movement “using the devices unique identification number (UID)”, Password-based attacks, Cyber-crimes [53].

2.5 Security issues according to IoT layers

As mentioned before that there are different layers in IoT. Each layer suffers from some kinds of cyber threats and security issues as shown in Fig. 3 [42, 113] and categorized as follows:



Senseing Layer	Network Layer	Middleware Layer	Gatwey	Application Layer
•*Node Capturing* •*Malicious Code Injection Attack* •*Side-Channel Attacks* •*Eavesdropping and Interference* •*Booting Attacks*	•*Phishing Site Attack* •*Access Attack* •*DoS/DoS Attack* •*Data Transit Attacks*	•*Man-in-the-Middle Attack* •*SQL Injection Attack* •*Cloud Malware Injection* •*Flooding Attack in Cloud:*	•*Secure Onboarding* •*Extra Interfaces* •*Firmware updates*	•*Data Thefts* •*Service Interruption Attacks* •*Access Control Attacks*

Fig. 3 Security issues based IoT layers [42]

- **Sensing layer**

- *Node Capturing:* Nodes are captured or replaced by other malicious nodes controlled by the attacker.
- *Malicious Code Injection Attack:* By injecting malicious codes in the memory of the devices to force them to perform some unintended functions or access the complete IoT system.
- *Side-Channel Attacks:* Like in electromagnetic attacks, power consumption, and timing attacks.
- *Eavesdropping and Interference:* where the attackers capture the data during the transmission or the authentication of the collected data.
- *Booting Attacks:* There is a risk at boot time that attackers may try to attack the node as the security processes of the device are not active until the device is fully booted.

- **Network Layer**

- *Phishing Site Attack:* where the attacker targets several IoT devices of the same owner. Once the attacker compromises the account and password of a user, then the entire IoT network that the user is part of becomes vulnerable to cyber-attacks.
- *Access Attack:* In which, an unauthorized person could be able to gain access to the network of IoT devices. The purpose of this kind of attack is to steal valuable information from the user.
- *DoS/DoS Attack:* in which a huge amount of unwanted requests is flooded to the target servers. If there are multiple sources used by the attacker to flood the target server, then it is termed as DDoS or distributed denial of service attack. Mirai botnet is an example [42].
- *Data Transit Attacks:* during transmission, the data is more vulnerable to cyber-attacks. Routing Attacks: where malicious nodes aim to redirect the routing paths during data transmission. Sinkhole and wormhole are types of this attack [42].

- **Middleware Layer**

- *Man-in-the-Middle Attack" MitM":* If the attacker can control the node, then s/he may have the ability to control all communication between participants.
- *SQL Injection Attack:* embedding malicious SQL statements in a program to obtain private data or alter the database.
- *Cloud Malware Injection:* The attacker creates a virtual machine to inject malicious codes in the form of malware.
- *Flooding Attack in Cloud:* like in the DoS attack which affects the quality of service (QoS).

- **Gateways**

- *Secure Onboarding:* by applying MitM attacks to capture the encryption keys of the nodes.
- *Extra Interfaces:* some unnecessary services should be restricted for end-users to prevent hackers from achieving backdoor authentication or information breach.
- *Firmware updates:* upon downloading and updating the firmware via gateways. The signatures and versions should be checked and recorded for secure firmware updates for more protection.

- **Application Layer**

- *Data Thefts:* to add more confidence to online users, some techniques should be used for private data protection such as encryption, and isolation of the data, user authentication, management of privacy can be used to secure IoT applications.
- *Service Interruption Attacks:* in this kind of attack authorized users cannot use the services of IoT applications as the attackers make the servers or network too busy to respond.
- *Access Control Attacks:* Once the attacker compromises the account and password of a user, then the complete IoT network that the user is part of becomes vulnerable to cyber-attacks.

3 IoT forensics

Digital forensics concerns gathering digital evidence then analyzing and examining them to find any traces related to criminalities against the digital systems. Digital forensics has several types such as Computer, Network, Mobile, IoT, and Cloud Forensics.

The first Digital Forensic Research Workshop (DFRWS) defined digital forensics as: "*The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or* *furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations*" [43, 84].

From the above definition, the digital forensic process for the investigation of cybercrimes can be as shown in Fig. 4 as follows [77]:

- **Identification:** To identify the evidence in a crime scene, that evidence will be used to prove the occurrence of an incident.
- **Preservation:** In this phase, the investigator isolates, secures, and preserves data.
- **Analysis:** In the analysis phase, the investigator construes and correlates evidence, to prove or disprove the incident.
- **Documentation:** In this phase, the investigator Documents the crime scene along with photographing, sketching, and crime-scene mapping.
- **Presentation:** In this phase, finally the investigator summarizes and explains the conclusions that are done with the help to gather facts.

In [109], authors mentioned that the digital forensics life cycle consists of 5 steps or phases: identification of evidence, evidence collection, recovery, analysis, and preservation of digital evidence

3.1 IoT Forensics Model

The combination of IoT and digital forensics led to the concept of IoT forensics which attracted multiple researchers' attention. The rapid growth of IoT devices and objects brings countless benefits but it came with new security and forensics challenges. IoT Forensics can be defined as the process of performing digital forensic investigation in the Internet of Things environment. This means collecting and analyzing digital evidence from the Internet of things infrastructure which includes all the parts of the IoT environment.

From the above definition of IoT Forensics, authors identify that the digital investigation process in the IoT could be done at three digital forensics levels as follows:

- **Bottom Level:** IoT Device Forensics level
- **Middle Level:** Cloud/Internet Forensics Level
- **Top Level:** IoT Application Forensics Level

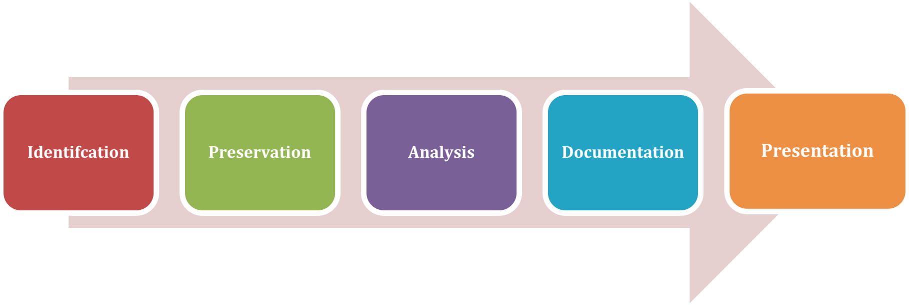


Fig. 4 Digital Forensic Investigation Process

These levels will be covered using basic forensic investigations phases which are identification, collection, preservation, examination, analysis, and presentation. The IoT Forensics Investigation process that can be followed to investigate crimes related to IoT is shown in Fig. 5. This model consists of four main phases, identification of digital evidence, data collection and acquisition, data analysis, and examination, and final report and presentation of a summary of the entire investigation process.

The concept of digital forensics has been applied in different domains; however, different IoT applications need adjusted investigation processes. The heterogeneity of IoT devices and objects should be taken into consideration when implementing any forensic model for the IoT. Traditional computer forensics is used to deal with the interconnected computers with the stored data on them with the general data format of electronic files with different file formats such as JPEG, MP3, etc.… IoT devices raise the challenges for forensics as they may exist at any geographical location, types of files are of any format as the devices are of different types; Home appliances, connected cars, wearable devices, RFID, sensors nodes, WSNs, and medical devices. These devices share data from various format. Table 2 shows a comparison between computer forensics and IoT forensics.

3.2 Requirements of IoT forensics

The massive amount of generated data of all IoT devices around the world makes it hard to adopt the traditional digital forensics investigation models. The wide variety of IoT devices will also raise a problem in data analysis because of the heterogeneous formats of data. For successful IoT forensics to be applied, there are a set of requirements should be ensured:

- Some IoT devices collect sensitive users' data regarding their habits, financial account, passwords, etc. These types of data will be used by the investigator in the case of cyber-

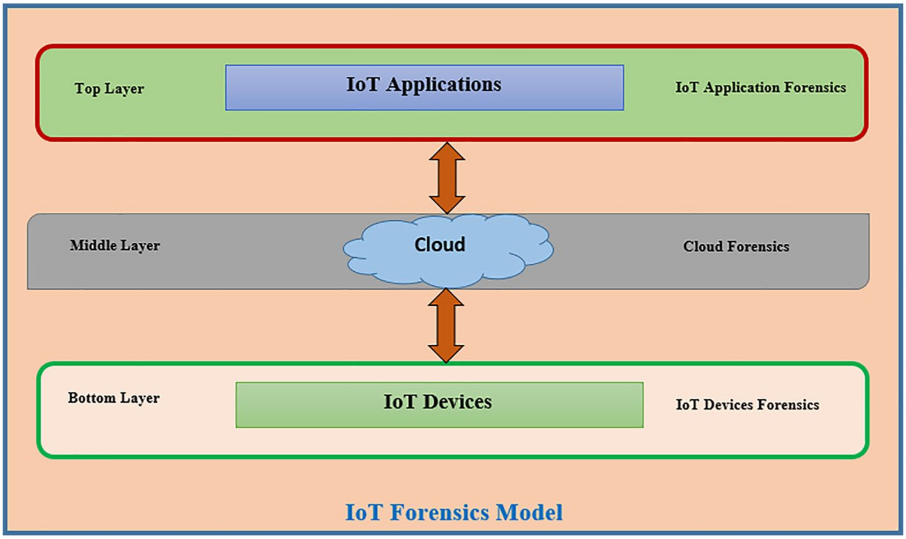


Fig. 5 IoT Forensic Investigation Model

Table 2 Comparison analysis between Computer and IoT Forensics

Item	Computer Forensics	IoT Forensics
Number of devices	Many billions of devices	It is expected to have 20.4 billion IoT devices by 2022 and it's increasing
Network boundaries	Relatively clearly defined boundaries and lines of ownership	There are no defined boundaries
Ownership	Governments, Individuals, companies, groups, etc	Governments, Individuals, companies, groups, etc
Evidence Source	PC, social networks, mobile devices, authentication, web clients, authorization, and accounting servers	Wearable devices, home appliances, connected cars, RFID, sensors, WSNs, and medical devices
Evidence Type	Standard file formats such as electronic documents, JPEG, MP3, etc	All files formats
What to seize	Seize devices as required	Identify the next best things for the source of evidence

crime. Therefore, users should be aware that their data is being used in the investigation process, and they should be aware of who accessed their data and used it for investigation. On the other hand, the investigators who access users' data must ensure maximum protection from unauthorized access, loss, and manipulation [80, 110, 126, 135].
- The amount of captured data via IoT devices and sensors from networks and the cloud raises several issues for the identification of relevant data for the investigation process. These data need to be managed properly to be effective evidence for an investigation. the process of collecting the data that is spread across different locations across countries complicates evidence collection because data can be mixed with other users.

While the IoT provides several sources of evidence for investigators and practitioners, there are a set of challenges that are stumbling blocks that prevent performing a successful forensic investigation in the IoT environment. These challenges can be as [39]:

- The collected digital evidence integrity is an important issue in digital forensics. Most digital forensic methods calculate a hash and maintain chain-of-custody to assure integrity. But in the IoT system, there is a lack of available tools that can prevent accidental evidence changes in the endpoint.
- In the forensic investigation of IoT systems, the process of documenting the topology of the endpoint's network is a complex challenge, as there are some possibilities that some sensors from the crime scene are sending information to IoT appliances residing at an unknown location.
- The main challenge in the IoT crime scene is evidence visibility, there are possibilities not to see the required endpoint in the crime scene, on the other hand, an investigator may even find hundreds of sensors embedded in any existing device in the crime scene. Sometimes it is not easy or even possible to check every inch in the crime scene. In this case, the investigator would better check the network logs to identify the number of sensors connected to the network under investigation.

In an ordinary crime, the weapon is tangible, so the investigators investigate the crime scene by tracking the attacker's fingerprints and activities to obtain a clear idea about what happened in the crime scene to identify the criminal. In digital crimes, the weapon is malicious code, so the investigator tries to track the criminal's digital traces on the local system, the network, or the Internet to uncover their digital identity [100].

3.3 Challenges of IoT Forensics

The challenges of IoT forensics can be as follows [44, 66, 94, 99, 100]:

- The data retrieval process needs experts to deal with heterogeneous IoT devices.
- Data on the devices are not synced with the cloud so the data retrieved may be incomplete
- The stored data on the cloud may store the previous event than the required event
- The limited storage of the devices prevent storing the whole event
- The cloud may store data for a limited period and delete the data after this period expires. The deleted data may be very important for the investigation.
- The device may explore devices on other networks than its networks making it harder for the investigator to identify the connected devices.

- Some devices cannot set up the software according to the limited resources
- Data on devices can be lost if powered off, while some devices keep logs of activities unless reset to factory settings.
- Wrong reconstructions of the events may lead to very dangerous wrong conclusions that may lead to charge innocent people
- Additional speech recognition tools are required to identify voice commands.
- Sometimes the voice commands are ordered remotely from other locations; where the criminal is not physically present at the crime scene.
- The evidence device may be used by someone else than its owner.
- The integrity of the collected data must be approved to avoid mistaken analysis.
- Some SSD devices delete data permanently if requested. That makes it hard to retrieve the data.
- Decrypting encrypted files.
- Acquiring user credentials to access data on the cloud.
- Acquiring a passphrase to stored files.
- Locating and decrypting shards on different nodes.
- Recovering sharded files from different storage nodes.
- Identifying a shard's geographical location.
- The huge quantity of data is mostly is either unstructured or not explicit.
- Data Acquisition Complexity: HDD is the simplest in data acquisition, then the encrypted data on HDD. Ram is more challenging as it loses its data if the device is turned off. Cloud storage is more difficult as it stores data around the country or even the world. If data is encrypted before it is uploaded and is stored in multiple computers becomes the hardest data acquisition.
- Improve the reliability and trustworthiness of evidence items in DF.
- With the massive amount of digital data from IoT devices, it is very hard to recognize which data is important for the investigation.
- If any errors occurred in the collecting phase, then it will affect all other phases and may lead to a different decision.
- Some devices work together over a non-IP network, and at the same time they deal with the cloud using IP; then it makes it harder to identify the devices
- Some IoT actuators are embedded by Real-time Operating Systems (RTOS); which means that they process data on non-volatile memory for faster actions. That raises the risk of losing logs if these devices are powered off.
- Mobile devices; such as cell phones and vehicles join different networks as they move. The forensic tools cannot deal with that dynamic topology.
- Not all IoT devices are embedded with tamper-resistant software; which prevents tampering with the systems by hackers.
- Some logs of IoT devices are not supported for forensic analysis; it doesn't include who, who, when, where, and why an incident was executed.

4 Blockchain technology

In last years, cryptocurrency is considered to work as a digital medium of exchange; that uses robust cryptography to confident financial transactions, control the creation of additional units, and verify the fund transfer. Bitcoin [117] was invented by Nakamoto as the first cryptocurrency. Bitcoins are based on the concept of Blockchain to enable reliable transactions in decentralized management. Steps in the cryptocurrency system can be as the next [29]:

- Generate a public key and private key for each user to have a wallet.
- The sender sends the coin to the receiver using the public key and signs it using his private key.
- Finally, the transaction is validated and added to the chain via the mining process.

Blockchain is considered as a distributed data structure; named ledger. Ledgers contain information about transactions of the participant nodes of IoT. The entries "blocks" in the data structure are stored by linking one to another in sequential order similar to a linked list. The database is replicated and shared among each node in the network [64, 92, 112]. Each transaction in the ledger must be authenticated or agreed upon by more than half of the devices in the network, to ensure that no single device would take the control of the ledger to delete, modify or even add any blocks without other nodes approval [12, 104, 112]. Blockchain is considered as the implementation layer of a distributed software system or purely peer-to-peer system in which all the interconnected nodes have the same authentications with no central control. All participant nodes have the same privileges to verify transactions or supply IoT data in a decentralized fashion [58, 92, 104, 112]. The decentralized fashion enables the sharing of computing power and limited resources of all devices increasing reliability. The most common drawbacks of Blockchain are communication overhead and latency according to mining [112].

4.1 Elements of blockchain

In [12], they mentioned the main elements of Blockchain to be: Transactions and Blocks. Transactions are the actions among the participant devices in the system. Blocks of the chain record the transactions in the correct sequence making sure they have not been tampered with. Each block is composed of four parts: transaction details, the present and previous blocks hash values, and timestamp [104]. [123] gives another structure of blockchain with three components; block to record the transaction, chain to link all blocks, and network which is the set of participant nodes of the chain. The genesis block is the first block of the chain and it contains the first transaction. All blocks in the Blockchain can be traced back to the genesis block. The previous hash is forwarded to the miner who uses it to compete with other miners to introduce the new blocks into Blockchain and generate the new block hash [112, 115]. Figure 6 shows the general architecture and components of the Blockchain. In figure nodes 1,2,…N are connected to construct the chain. If node 4 transfers transaction to node 5 "the red arrow" then node 4 constructs a block with the shown components; header and transaction. The block then is mined and added permanently to the chain. Each block can be traced back to block 0; genesis block.

According to [93] there are four main functionalities in Blockchain:

- The routing function, which is responsible for propagating transactions and blocks among network participants.
- Each participant node has a complete copy of the chain.
- Users are granted public and private keys from wallet services to operate with the chain: "Bitcoin in case of financial application".

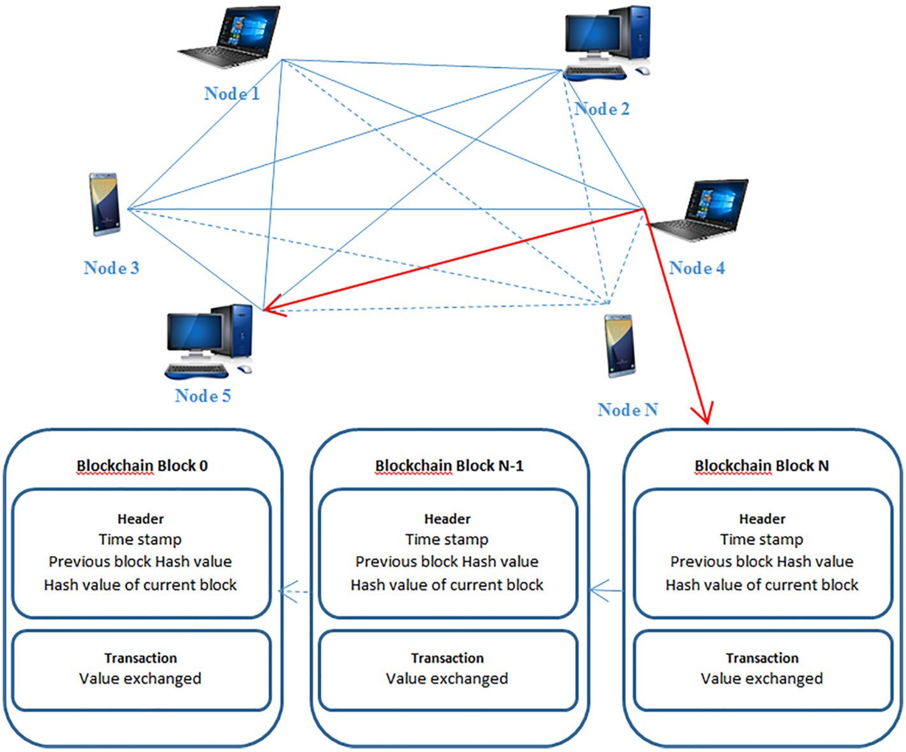


Fig. 6 Blockchain archetitcture and components

- The mining function is the function in which nodes validate new blocks and add them to the chain via proof of work (POW) or other consensus protocols.

The types of nodes in IoT Blockchain are:

- **Full nodes:** they store the entire Blockchain to validate transactions and blocks during mining.
- **Lightweight nodes:** they have only part of the Blockchain, they are easier to run and maintain than full nodes.
- **Full nodes miners**: the nodes that have more resources than others and they can contribute invalidating the transactions and solve hash puzzles; consensus algorithms [93].

4.2 Characteristics of blockchain

There are several characteristics for Blockchain as the following: [12, 42, 58, 92, 93, 104, 115, 123]

- **Decentralization:** Unlike traditional centralized systems, Blockchain has no central authentication for transactions. Any participant node can validate the transaction before being added to the chain by solving the Proof of Work (PoW) puzzle. In centralized systems, there are some possible scenarios where a few companies with more powerful resources control the processing and storage of people's information. This decentralized manner of Blockchain prevents causing a bottleneck and a single point of failure. The transactions in Blockchain must be verified by the majority of participants to add them to the distributed ledger.

- **Anonymity:** The participant devices of the Blockchain have a public/private key, which does not reveal their real identity.
- **Autonomy:** Blockchain nodes can interact with each other without the involvement of any servers.
- **Security:** Blockchain can secure communication and message exchange among nodes using smart contracts. It prevents unauthorized data access and data loss by ensuring that only nodes with appropriate public and private keys can access, decrypt, and encrypt data.
- **Non-repudiation.** The Blockchain ensures that: transactions can be easily validated; and once the transaction is validated and added as a block to the chain, it cannot be deleted or rolled back.
- **Resiliency:** Each node has a copy of the ledger that prevents having a single point of failure.
- **Smart contracts:** They are software programs that specify contracts among two or more participants. They have the advantages of cost reduction, speed, precision, efficiency, and transparency. The content of the smart contract is trusted among nodes as it cannot be modified or corrupted. Each smart contract is stored in the chain and is given a unique address and the transactions are sent to that address to invoke the contract to run the appropriate action based on the code.
- **Auditing:** During the change of ownership of a certain device, Blockchain can record time, location, price, parties involved, and other relevant information. Blockchain can also be used to record all the information of the device throughout its lifetime including updates, patches, and part replacements.
- **Immutability:** Immutability on the contrary of centralized systems "which can be corrupted", the Blockchain ledger is immutable once the transaction is verified no changes are allowed to be done to it. Moreover, decentralized technology enables sensor data traceability and accountability.
- **Capacity:** As the Blockchain shares the resources of millions of participant devices and by using a proxy server that stores the resources in an encrypted form until needed.
- The cryptographic algorithms used by Blockchain would endure data privacy and prevent unauthorized devices from capturing data even if they have fake access to the chain the actual data needs keys to be viewed.
- **Publicity:** All IoT devices have their copy of the ledger so they can see all the transactions and all blocks. The content of the transaction is protected by the private key of the device.
- **Speed:** A Blockchain transaction is validated and distributed across the network in minutes.
- **Cost-saving:** Due to the use of decentralized architecture and share resources among participants where it can use to store and transmit a huge amount of sensed data.

4.3 Challenges of blockchain

Blockchain poses many challenges as follows: [93, 115]

- **Storage capacity and scalability:** the chain growth rate is 1 MB per block every 10 min in Bitcoin. There is a copy of the ledger stored at each node in the network. As the size of the chain grows, nodes require more storage and processing resources. Compression and cloud integration can solve the problem.
- **Security:** weaknesses and threats:
  - *51% attack:* This attack can occur if a node in the Blockchain can access control of more than 51% of the mining power, controlling the consensus in the network it is also known as a *majority attack*. to solve this problem, solo mining incentives or P2P mining could be applied [14].
  - *Double-spend attack:* this kind of attack refers to spending the same coin more than once. In Bitcoin for example a transaction is considered to be confirmed only if it is stored in a block in the Blockchain. This process takes between 20 to 40 min which brings high latency to the chain [142].
  - *Race attacks:* It is the situation where a user sends a transaction directly to the merchant, and the merchant accepts the transaction before the required time of transaction validation. The same user may probably re-transfer the same paid amount to himself. The second transaction may be confirmed first, and the merchant is cheated [93].
  - *Denial of Service (DoS):* The DoS [107] attacker floods the targeted servers with a huge amount of unwanted requests. In the case of using multiple sources to flood the servers, then it is called a Distributed Denial of Service (DDoS) attack. The Mirai botnet [3, 119] is an example.
  - *Man in the Middle (MitM):* If the attacker can control the node, then he/she can get complete control of the chain communication [59].
- **Data privacy:** data in the Blockchain can be encrypted using multiple types of encryptions. Some examples are: Hawk [57], Enigma project [147], Quorum [16], Multichain[128], Rockchain[50].

4.4 Blockchain types

The Blockchain is categorized as tabulated in Table 3 and applied differently according to the domains.

Table 3 Domain-based Blockchain Systems

Feature	Consortium	Private	Public
Access to data	Authorized users	Authorized users	Anyone
Network expansion	Easy	Very easy	Difficult
Proof of transaction	Previously agreed rule	Central agency	Verification algorithm
Identifiability	Possible to identify	Possible to identify	Anonymity
Transaction speed	Fast	Fast	Slow
Transaction maker	Only authorized users	Only authorized users	Everybody

4.5 Consensus protocols in blockchain

They are the basic feature behind the security and performance of Blockchain [130, 143]. They are algorithms that determine how a transaction can be added to the ledger. Consensus protocols are used to guarantee the trustworthiness “of a Blockchain by preventing 51% and double-spend attacks. The new block must be approved by the majority of nodes before it can be appended to the Blockchain. Using hashes ensures that the blocks are not tampered with as any change in any existing block would produce a different hash value.

There are many protocols such as Leased Proof of Stake (PLoS), Proof of Burn (PoB), Proof of Authority (PoA), Elapsed Time Test (PoET), Proof of Understanding (PoU), Paxos, Proof of Capacity (PoC), Chubby, RAFT, proof-of-importance (PoI), Practical Byzantine Fault Tolerance (PBFT), SIEVE Stellar HDAC. In [143], they provided a study of different consensus protocols. Some of the most used Consensus protocols in Blockchain are:

- **Proof-of-work (PoW):** It is an energy-consuming algorithm used to maintain and validate the Blockchain through hard-to compute, but easy-to-verify, computational puzzles. Used by NameCoin, LiteCoin, Ethereum, DogeCoin, and Monero [60].
- **Proof-of-Stake (PoS):** in this algorithm participants of the blocks validation are chosen according to the number of coins they own [97].
- **Delegate PoS (DPoS):** Each time a node successfully produces a block is rewarded [134]. Used by BitShares; where the participants of the blocks validation are chosen by voting, Monax, Lisk, or Tendermint.
- **Practical Byzantine Fault Tolerance (PBFT):** The (leader) is changed every round and each round includes 4 phases:

  (a) The client node sends requests to the leader node.
  (b) The leader node multicasts the request to the backup nodes.
  (c) The nodes then execute the request and send a reply to the client.
  (d) The client node receives m + 1 replies from different nodes with the same answer, and the client gets the requested data.

The advantages and disadvantages of the mentioned four consensus algorithms are presented in Table 4 [124].

5 Blockchain-based IoT security and forensics

The IoT security can be enhanced by leveraging the Blockchain technology based on the following issues as shown in Fig. 7:

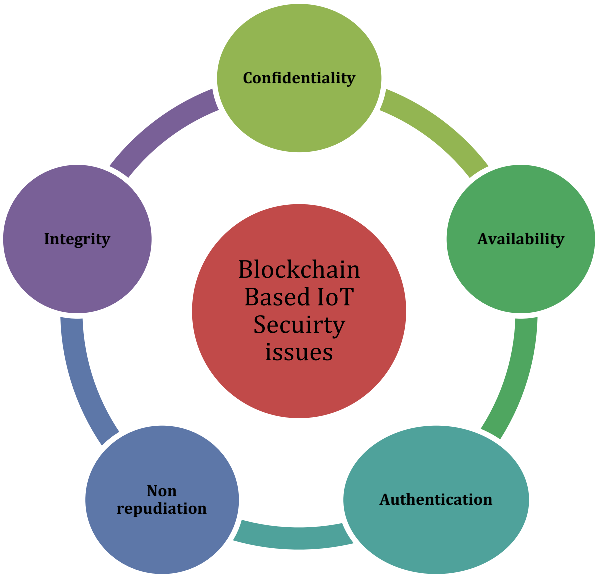
- **Confidentiality:** It represents how to protect the user’s info. It denotes that accessing data by any person should be controlled in the way that only the intentional receiver can access that data. For IoT Confidentiality, the data stored on the Blockchain can be encrypted, the pointer to the data location is then sent to the intentional receiver. The recipient’s public key is used to encrypt the decryption key before transferring it to the recipient.

Table 4 Advantages and disadvantages of consensus algorithms [124]

Consensus Protocols	Pros	Cons
PoW	• Safe and stable, a high degree of freedom of nodes • A high degree of decentralization, open node system	• Weak scalability and low performance • Causing hardware equipment waste
PoS	• Less energy • A high degree of decentralization, open node system	• Complex implementation process • Security breach
DPoS	• Less energy • High performance • Finality	• Weak degree of decentralization closed node system
PBFT	• Higher performance • Finality • High security	• Weak degree of decentralization, the closed node system • Low fault tolerance

- **Authentication:** Customary authentication systems are not suitable for IoT because they are too complex for resource-constrained IoT devices. A decentralized Blockchain-based authentication scheme can be used for IoT authentication for registering and verifying the identities of all IoT devices. So, Blockchain can be used in signing, verification, encryption, and decryption in smart IoT-based Applications.
- **Availability:** Blockchain is considered as a distributed and public ledger, that can be used to securely store and transfer IoT data as well as make it reliably available at all times.
- **Integrity:** In Blockchain, the integrity of the data or transactions is preserved based on both hash functions and Merkle trees. Therefore, any change in the data could change the hash values, which provides data integrity.

Fig. 7 Blockchain based IoT Secuirty Issues



- **Nonrepudiation:** To guarantee that the sender cannot deny it has produced the data. This concept is called Nonrepudiation. In Blockchain, each transaction is signed by the sender before being added to the Blockchain network. The transactions and blocks are hashed to avert altering and ease auditability. Therefore, the sender cannot deny creating specific data. In the IoT infrastructure, it is required to audit the status of real-time data. The Blockchain will enable the user to exactly identify the time and location of any illegal events to modify the data.

From existing studies, it concluded that there are limitations and challenges in the integration of Blockchain and the Internet of Things as shown in Fig. 8 as the following:

- **Scalability:** In the present enactments of the Blockchain, an upsurge in the node's number would lead to noteworthy scalability issues because of high processing overheads. IoT already suffers from scalability issues, which would affect a Blockchain-based IoT convergence. This problem desires to be resolved to enhance the complete system performance.
- **Storage:** Blockchain eradicates the necessity for a central server for data/transactions storage. Though, the global ledger is replicated and stored on the nodes' local storage. The notable growth of the ledger size according to adding more blocks makes it difficult for the low storage capacity IoT devices to store the whole ledger.
- **Blockchain Platforms:** A Blockchain-based IoT application depends on the platform it is being executed on. All the shortcomings of their platform such as throughput and latency would affect the applications.
- **Processing Power and Time:** The cryptographic methods and consensus procedures employed in Blockchain need significant processing resources, which exceed the abilities of most IoT devices.
- **Consensus Procedures:** Consensus protocols required for blockchain implementation such as PoW and PoS are energy-consuming and need processing resources that exceed the abilities of most IoT devices.

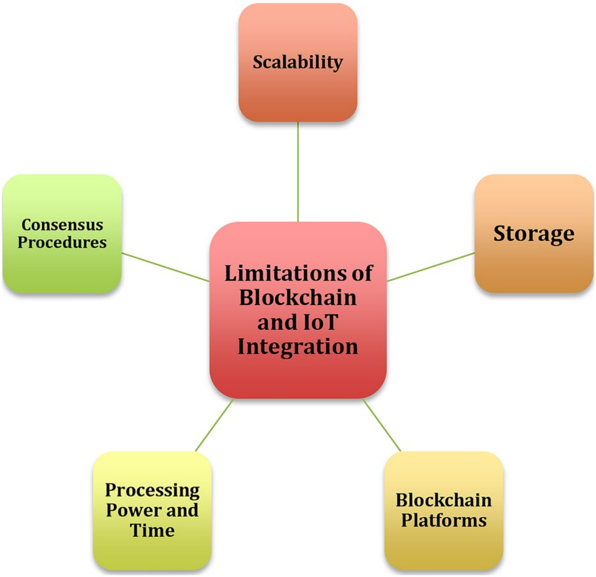

Scalability
Consensus Procedures
Storage
Limitations of Blockchain and IoT Integration
Processing Power and Time
Blockchain Platforms

Fig. 8 Limitations of the integration of Blockchain and Internet of Things

From the challenges facing the IoT forensics; mentioned in Sect. 3, and the characteristics of Blockchain; mentioned in the previous section a combination between blockchain and IoT forensics can eliminate various issues to facilitate the investigator's mission. Some recent researchers built Blockchain-based IoT forensic frameworks to benefit from the decentralization, data integrity, and immutability, and security characteristics of blockchain. Some of them are briefly presented while Table 5 presents a summary of the used papers for this work.

Authors in [94] proposed a decentralized cloud storage system called STORJ. The process is as follows: First, each file is encrypted using SHA256-CTR and split into smaller 8 or 32 MB files. These new smaller files are combined to form a shard, with any extra space is padded. The resulting shards are then salted, hashed, and transmitted to the network. The authors designed a windows application to enable users to allocate the available disk space to be used for renting. Each user has to create a Bitcoin address to receive the STORJ Coin. They collected file shards for a month for the experiment. From the transactions, they could identify some interesting items that could be used in a forensic investigation as contract numbers in hexadecimal format, signature, and the payment destination. Authors in [99] proposed their methodology for smart home forensic analysis, which is applied in six steps:

- *Preliminary analysis:* To make a brief study of the device to provide information about traces and vulnerabilities on the device and gives knowledge about how to gain root access to the device.
- *Testbed setup:* The device is tested in a controlled environment to enable the passive collection of all traffic performed by the device and test possible attacks on the device.
- *Network analysis:* to study with whom the device communicated, which protocols are used for communication, and whether any readable information is transmitted or not.
- *Smartphone application analysis:* As the smart home systems are monitored using smartphone apps; it is important to study these apps to uncover additional information like the user's commands that are sent within the test environment.
- *Vulnerability analysis:* this step aims to figure out how an attacker can compromise a device, as well as to discover how to acquire data from the device.
- *Physical analysis:* To investigate the IoT device to get access to the device's memory and storage to retrieve important information about the activities of its owner.
- *Cloud:* The stored data on the cloud needs Legal authorization to be obtained to be used in forensic investigation.

Authors in [66] presented a new Blockchain-based framework for a forensic investigation called IoTFC. They aim to reduce the cost and time of the investigation. The first categorized the evidence into five grades according to the identification difficulties:

Grade 1: Easy to identify like plain texts and unencrypted files.
Grade 2: The files that are modified in their extensions to make them un-openable.
Grade 3: Hard to identify; these files are written in plain text and not stored in the files system and volume slack.
Grade 4: Difficult to identify: represented by encrypted data or password-protected files.
Grade 5: Very difficult to identify as files with steganography.

Table 5 A Summary of Blockchain-based IoT-forensic existing work

Research Work	Year	Contribution Summary
[94]	2019	The paper proposed a decentralized cloud storage system based on Blockchain named STORJ
[99]	2019	The work proposed a new 6-steps methodology for smart home forensic analysis
[66]	2019	The research proposed a new Blockchain-based framework for a forensic investigation called IoTFC to reduce the cost and time of the investigation
[44]	2018	The paper proposes a forensic investigation framework for IoT "FIF-IoT" based on Blockchain
[20]	2019	The paper proposes a Blockchain-based application for evidence preservation; Cyber Trust Blockchain “CTB” using hyper ledger fabric
[131]	2019	The work proposed another electronic evidence preservation model based on Blockchain (EEPM)
[35]	2019	The paper proposed a new model for triage the electronic evidence in the crime scene. This model is called a SEAKER (Storage Evaluator and Knowledge Extraction Reader)
[74]	2020	The paper proposed a Cost-efficient IoT Forensics Framework with 2 layer Blockchain
[26]	2020	The work proposed Blockchain Solutions for Forensics. Some types of forensics and challenges of them with some blockchain-based possible solutions
[129]	2020	The paper proposed a Lightweight Mining mechanism to mine new blocks in the blockchain with less computational power
[75]	2020	The paper proposed a Cost-efficient IoT Forensics Framework with Blockchain. to verify the authenticity and integrity of the data collected from various IoT devices for more security and tamper-resistance systems
[103]	2020	an overview of the application related to the construction industry based on Blockchain with IoT infrastructure
[56]	2020	The paper proposed a lightweight and tamper-proof event log for the IoT system based on blockchain
[45]		The paper proposed a log storage management protocol based on blockchain for IoT
[65]	2020	The paper proposed LEChain; a blockchain-based lawful evidence management scheme to supervise the entire evidence flow to prevents malicious investigators from counterfeiting the evidence
[9]	2020	The paper proposed a model for securing management of IoT devices based on blockchain

The steps of the IoTFC can be as the following:

1. **Evidence identification and acquisition:** identification of the digital evidence, add fingerprint and timestamp to it, add the evidence to the chain allowing all participants to view and share a copy of the forensic chain.
2. **Analysis:** using smart contracts to create analysis results some additional analysis tools are used like LogRhythm, EnScript of EnCase.
3. **Presentation:** all reports and findings are based on the Blockchain and appended to the chain.

Authors in [44] propose a forensic investigation framework for IoT "FIF-IoT". They first identified the challenges related to the IoT environment in each step of digital forensics,; Evidence Identification, Evidence Collection, and Acquisition, Evidence Organization, Evidence Examination. They divided interaction types among IoT-based systems into three categories: 1- Things to Users (T2U). 2- Things to Cloud (T2C). 3- Things to Things (T2T). They used a public digital ledger "blockchain" to store interactions among (clouds, users, and IoT devices) as evidence. Their system eliminates the single entity's control and single-point-of-failure on the storage. FIF-IoT ensures anonymity, integrity, non-repudiation, and confidentiality, of the stored evidence in the ledger. Furthermore, it provides a mechanism to acquire evidence from the ledger and a mechanism for integrity verification of these evidence. They applied their system to the medical case; a patient with acute diabetes.

Authors in [20] propose a blockchain-based application for evidence preservation; Cyber Trust Blockchain "CTB" using hyper ledger fabric. Their model stores the metadata of the electronic evidence, while the evidence is stored in a separate cloud server. That metadata includes (user ID, evidence creator, evidence description, action timestamp, the current owner of the evidence, previous owner of the evidence, evidence type, and time records list). They store the electronic evidence in the database ev_DB. They are grant authentications for three types of entities to deal with electronic evidence. 1- Internet Service Providers "ISP"; who are data collectors and they have permission to delete the evidence if required. 2- Low Enforcement Agency (LEA); which can access the evidence using their IDs and issue new transactions to the chain. 3- Prosecutor; they are the final owner of digital forensic evidence.

Authors in [131] proposed another electronic evidence preservation model based on Blockchain (EEPM). Their model stores only the hash value and metadata of the evidence in a Blockchain manner. Four parts of the data are presented and processed in their model. 1- Part (1): is the complete information about the evidence. 2- Part (2): is the information about system users. 3- Part (3): a platform for business data. 4- Part (4) is log data (independent of the system to store). The model stores the metadata of the electronic evidence and the evidence themselves I separate storage places to enhance security. The evidence database is backed up to guarantee failure and/or loss recovery of evidence.

Authors in [35] proposed a new model for triage the electronic evidence in the crime scene. Triage is the first step in reviewing the scene devices to identify which devices have to be investigated deeply. Their model is named Storage Evaluator and Knowledge Extraction Reader (SEAKER). They use a Raspberry device embedded with Wi-Fi and USB ports to establish a hotspot to connect all existing devices in the crime scene to it. Some predefined patterns" for file names and extensions" are identified and the devices are scanned in read-only mode for these patterns. If one or more patterns are found on a device then it is taken to the labs for deeper investigations. Otherwise, the device is left behind. They argued that their model is inexpensive, easy to use, and quick. Some improvements have to be applied to the model as the authors' opinion: 1-the system cannot identify which file is for which device if more than one device is attached to the Raspberry device. 2-the system cannot deal with some file systems of the device.

But in our opinion, the most critical issues of this system are:

- Not all possible patterns used by the cybercriminals can be predefined in this case very valuable evidence can be missed.
- All devices in the scene must be considered as evidence and have to be preserved for careful investigation.

Authors in [74] proposed A Cost-efficient IoT Forensics Framework with Blockchain. They argued that the model is cost-efficient and more secure. They save incident information in both cheaper EOS and Stellar chains before writing a daily summary to the Merkle tree; thus their application is two-layer blockchain-based. Second, in case of a 51% attack attacker must hack both EOS and Stellar within the same day before the summary is written to Ethereum; which is hard to be done, which makes the model more secure. They applied their model in a boat rental application. The boats are embedded by sensors. The application collects data for insurance purposes. Not all data are stored for storage saving. The data is filtered to determine the important data to be stored. They presented a future improvement suggestion by including additional low-cost blockchain platforms to increase the resistance against possible attacks.

Authors in [26] proposed SoK (Blockchain Solutions for Forensics). In their paper they mentioned some literature about some types of forensics; Cloud forensics, Data management forensics, Healthcare forensics, IoT forensics, Mobile forensics, Multimedia forensics, Smart grid forensics, Intelligent Transportation Systems forensics. They also mentioned some limitations of different types of Blockchain; public and private blockchain. They finally classified digital forensics challenges in six domains with some blockchain-based solutions for them. These challenges are:

- Tokenization of artifacts from digital evidence,
- effective data volume management in the chain of custody.
- Analysis of forensic procedures in Blockchain systems.
- Enable an intelligible outcome/reports from the forensic process.
- Interoperability and cross-border jurisdictions.
- Timeline of events and chronology.

In [129] authors proposed a Second-Generation Blockchain Technology with Lightweight Mining for Secure Provenance and Related Applications. Their work is to reduce the computational power required for mining new blocks in the blockchain. That would enable a faster, more scalable, and Environmentally friendly alternative than the well-known resource-intensive mining protocol; Proof-of-Work (PoW) which is used by Bitcoin for a permissioned. They applied for their work on 3 use cases; Academic Integrity, Digital Forensics, and Secure Logging. The authors claim that the Scrybe outperforms other systems regarding data integrity, non-repudiation, and DDoS attacks.

Authors in [75] proposed A Cost-efficient IoT Forensics Framework with Blockchain. Based on the boat rental application. Their framework consists of two layers- multiple blockchain networks used to verify the authenticity and integrity of the data collected from different IoT devices for more security and tamper-resistance systems. For reducing the size of the data, they utilized hashes and Merkle trees to store only the hash of hashes of the collected data. Where each boat is equipped with an onboard IoT edge to collect data about boat location In [103] an overview of the application related to the construction industry based on Blockchain with IoT infrastructure. Where smart contracts can be implemented to maximize productivity, the project management model can minimize late payments. The collected data through the participant industrial sensors and actuators are secured via Blockchain to solve privacy and protection issues in IoT applications.

Authors in [56] aimed to create a secure, lightweight, and tamper-proof event log for the IoT system based on blockchain. Their model stores Event logs from IoT devices and sends them "optionally encrypted using AES-256 Encryption on the server-side" to different servers using multiple communication channels for availability purposes. Their model consists of two single-board microcontrollers to gather data from embedded ultrasonic sensors. These sensors send data to single-board computers via USB serials. After being processed each event is sent as a blockchain transaction to each remote server via HTTPS. The log data are stored in the blockchain.

In [45] the authors proposed a log storage management protocol based on blockchain for IoT. They aim to store the logs that record important contents and private information. Their model allows sensors to encrypt the collected logs before sending them to the gateway and server. The system model includes 11 roles: attribute authority, SSO server, timestamp server, sensor (IoT device) and agent, gateway, blockchain server, private blockchain, public blockchain, storage cluster, and user. And is carried out including 13 phases: initialization phase device registration phase, SSO registration phase, SSO login phase, SSO password generation phase, user registration phase, log signcryption phase, log verification phase, private block calculation phase, private block verification phase, log unsigncryption phase, public block calculation phase, and public block verification phase.

Authors in [65] proposed LEChain; a blockchain-based lawful evidence management scheme to supervise the entire evidence flow to prevents malicious investigators from counterfeiting the evidence. They utilize randomizable signatures to authenticate witnesses' identities for their privacy. Then, they used ciphertext-policy attribute-based encryption for evidence access, to protect juror privacy, the authors designed a secure voting method. All evidence transactions are stored in consortium blockchain as well. Authors in [9] proposed a model for securing the management of IoT devices based on blockchain. Where the participant devices can verify their manufacturers, owners, users, and the actions or data they are taking.

It is observed from this study, there is a little research work focusing on Blockchain-based IoT forensics. Taking into account the limitation of both technologies, more researches have to be performed to enhance and improve the performance of IoT forensic via Blockchain technology.

6 Conclusion and open research points

Presently, no doubt that the Internet of Things (IoT) will transform our daily lives. IoT faces some serious cybercrimes investigation challenges with the billions of IoT transactions and devices. Therefore, this paper provides a study on the challenges and opportunities of applying Blockchain to assist digital investigators in performing cybercrimes investigation in IoT infrastructure in a forensically sound and timely fashion manner. Blockchain itself needs significant research efforts to adapt the computation-intensive algorithms to the limitations of energy and processing of IoT devices and the high latency of transaction approval at high scale networks.

As future open points in this interesting subject, there is plenty of open research work as follows:

- Provide new training methods for digital investigators to deal with a huge amount of evidential data in actionable time.
- Creating novel frameworks and models for the investigation of cybercrimes using classification and predations methods.
- Using the help of Blockchain in building accurate models for real-time fraud detection of criminals especially the finance sector.
- Build a cloud-based processing environment for handling massive data using big data platforms such as Apache Hadoop and Apache Spark.
- How to combine Blockchain and IoT technologies based on their requirements. By considering developing a set of protocols that can support the crucial requirements of entirely IoT applications instead of presenting application-specific IoT networks.
- Explore big data and Blockchain relationships and how the Blockchain can easily cover the flaws of big data.

References

1. Abomhara M (2015) Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. J Cyber Secur Mobil 4(1):65–88
2. Adhikary T et al (2019) “The Internet of Things (IoT) Augmentation in Healthcare: An Application Analytics.“ International Conference on Intelligent Computing and Communication Technologies. Springer, Singapore
3. Ahmed Z et al (2019) Protecting IoTs from Mirai Botnet Attacks Using Blockchains. 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD). IEEE
4. Albataineh A, Izzat A (2019) IoT and the Risk of Internet Exposure: Risk Assessment Using Shodan Queries. 2019 IEEE 20th International Symposium on” A World of Wireless, Mobile and Multimedia Networks“(WoWMoM). IEEE
5. Alam MM et al (2018) A survey on the roles of communication technologies in IoT-based personalized healthcare applications. IEEE Access 6:36611–36631
6. AlHammadi A et al (2019) “Survey of IoT-Based Smart Home Approaches.“ 2019 Advances in Science and Engineering Technology International Conferences (ASET). IEEE
7. Alhanahnah M, Stevens C, Bagheri H (2020) Scalable analysis of interaction threats in iot systems. Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis
8. Alhasnawi BN, Jasim BH (2020) Internet of Things (IoT) for Smart Grids: A Comprehensive Review. J Xi’an Univ Archit 63:1006–7930
9. Arcenegui J, Arjona R, Baturone I (2020) Secure Management of IoT Devices Based on Blockchain Non-fungible Tokens and Physical Unclonable Functions. International Conference on Applied Cryptography and Network Security. Springer, Cham
10. Arefin ASMS, Nahiyan KMT, Rabbani M (2020) “The Basics of Healthcare IoT: Data Acquisition, Medical Devices, Instrumentations and Measurements”. In: A Handbook of Internet of Things in Biomedical and Cyber Physical System. Springer, Cham, pp 1–37

11. Ashokkumar M, Thirumurugan T (2018) “Integrated IOT based design and Android operated Multi-purpose Field Surveillance Robot for Military Use.“ International Conference for Phoenixes on Emerging Current Trends in Engineering and Management (PECTEAM 2018) Atlantis Press
12. Atlam HF et al (2018) Blockchain with internet of things: Benefits, challenges, and future directions. Int J Intell Syst Appl 10(6):40–48
13. Badotra S et al (2020) (“IoT-Enabled Healthcare Network With SDN.“ 2020) 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). IEEE
14. Bae J, Lim H (2018) Random Mining Group Selection to Prevent 51% Attacks on Bitcoin.“ 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Workshops N (DSN-W). IEEE
15. Balakrishna S et al (2019) A Survey on Semantic Approaches for IoT Data Integration in Smart Cities. International Conference on Intelligent Computing and Communication Technologies. Springer, Singapore
16. Baliga A et al (2018) Performance evaluation of the quorum blockchain platform. arXiv preprint arXiv:1809.03421
17. Bansal A, Ahirwar MK, Shukla PK (2018) A Survey on Classification Algorithms Used in Healthcare Environment of the Internet of Things. Int J Comput Sci Engineering 6(7):883–887
18. Bao J, Hamdaoui B, Wong W-K (2020) IoT device type identification using hybrid deep learning approach for increased IoT security. 2020 International Wireless Communications and Mobile Computing (IWCMC). IEEE
19. Brignoli MA et al (2020) Combining exposure indicators and predictive analytics for threats detection in real industrial IoT sensor networks. 2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT. IEEE
20. Brotsis S et al (2019) Blockchain solutions for forensic evidence preservation in IoT environments. 2019 IEEE Conference on Network Softwarization (NetSoft). IEEE
21. Bui KHN, Jung JJ (2019) ACO-based Dynamic Decision Making for Connected Vehicles in IoT System. IEEE Transactions on Industrial Informatics
22. Burmaoglu S, Saritas O (2019) and Haydar Yalcin. “Defense 4.0: Internet of Things in Military.“ Emerging Technologies for Economic Development. Springer, Cham, pp 303–320
23. Catarinucci L et al (2015) An IoT-aware architecture for smart healthcare systems. IEEE Internet Things J 2(6):515–526
24. Chen J et al (2019) Your IoTs Are (Not) Mine: On the Remote Binding Between IoT Devices and Users. 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). IEEE
25. Cohen AE et al (2018) “Radio Frequency IoT Sensors in Military Operations in a Smart City.“ MILCOM 2018–2018 IEEE Military Communications Conference (MILCOM). IEEE
26. Dasaklis TK, Casino F, Patsakis C (2020) SoK: Blockchain Solutions for Forensics. arXiv preprint arXiv:2005.12640
27. Deepika K, Usha J (2020) Implementation of Personnel Localization & Automation Network (PLAN) Using Internet of Things (IoT). Procedia Computer Science 171:868–877
28. Dragičević T, Siano P, Prabaharan SR (2019) Future Generation 5G Wireless Networks for Smart Grid. A Comprehensive Review. Energies 12(11):2140
29. Easley D, O’Hara M, Basu S (2019) From mining to markets: The evolution of bitcoin transaction fees.“ J Financ Econ
30. Ejaz W et al (2019) Unmanned Aerial Vehicles enabled IoT Platform for Disaster Management. Energies 12(14):2706
31. El-Din HE, Manjaiah DH (2017) Internet of Things in Cloud Computing. In: Acharjya D, Geetha M (eds) Internet of Things: Novel Advances and Envisioned Applications. Stud Big Data 25. Springer, Cham
32. Fahmi F et al (2020) Integrated Car Telemetry System Based On Internet Of Things: Application And Challenges. J Eng Sci Technol 15(6):3757–3771
33. Farooq M, Shoaib et al (2020) Role of IoT Technology in Agriculture. A Systematic Literature Review. Electronics 9(2):319
34. Gandhi DA, Ghosal M (2018) “Intelligent Healthcare Using IoT: A Extensive Survey.“ 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT). IEEE
35. Gentry E et al (2019) SEAKER: A tool for fast digital forensic triage. Future of Information and Communication Conference. Springer, Cham

36. González-Zamar M-D et al (2020) IoT technology applications-based smart cities: Research analysis. Electronics 9.8:1246
37. Goudos SK et al (2019) Communication Protocols for the IoT-Based Smart Grid. IoT for Smart Grids. Springer, Cham, pp 55–83
38. Gupta BB, Quamara (2020) An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. Concurr Comput Pract Exp 32:e4946 21)
39. Harbawi M, Varol A (2017) An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework. 2017 5th Int Symp Digit Forensic Secur ISDFS 2017 520–525
40. Harish KV, Amutha B (2018) Survey on Security in Autonomous Cars. International Conference on Communications and Cyber Physical Engineering (2018) Springer, Singapore
41. Hassan WH (2019) Current research on Internet of Things (IoT) security: A survey. Comput Netw 148:283–294
42. Hassija V et al (2019) “A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. " IEEE Access 7:82721–82743
43. Hemdan EED, Manjaiah DH (2017) Digital Investigation of Cybercrimes Based on Big Data Analytics Using Deep Learning. Deep Learn Innov Convergence Big Data 9
44. Hossain M, Karim Y, Hasan R (2018) FIF-IoT: A forensic investigation framework for IoT using a public digital ledger. 2018 IEEE International Congress on Internet of Things (ICIOT). IEEE
45. Hsu C-L, Chen W-X, Tuan-Vinh L (2020) An Autonomous Log Storage Management Protocol with Blockchain Mechanism and Access Control for the Internet of Things. Sensors 20(22):6471
46. Hu X et al (2020) An IoT-Based Cyber-Physical Framework for Turbine Assembly Systems. IEEE Access 8:59732–59740
47. Huang S et al (2020) Identifying physical-layer attacks for IoT security: An automatic modulation classification approach using multi-module fusion neural network. Phys Commun 43:101180
48. Humayun M et al (2020) Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arab J Sci Eng 1–19
49. Janarthanan T, Bagheri M, Zargari S (2021) IoT Forensics: An Overview of the Current Issues and Challenges. Digit Forensic Investig Internet Things (IoT) Devices 223–254
50. Jehan S (2017) Rockchain A distributed data intelligence platform White Paper Beta 1.1 Sébastien Jehan
51. Jiang X, Lora M, Chattopadhyay S (2020) An experimental analysis of security vulnerabilities in industrial IoT devices. ACM Trans Internet Technol 20(2):1–24
52. Jiao S, Lui RP (2019) A survey on physical authentication methods for smart objects in IoT ecosystem. Internet Things 6:100043
53. Khan NS, Chishti MA, Saleem M (2019) Identifying Various Risks in Cyber-Security and Providing a Mind-Map of Network Security Issues to Mitigate Cyber-Crimes.“ Proceedings of 2nd International Conference on Communication, Computing and Networking. Springer, Singapore
54. Khoa TA et al (2020) Designing Efficient Smart Home Management with IoT Smart Lighting: A Case Study Wirel Commun Mob Comput 2020
55. Kimani K, Oduol V, Langat K (2019) Cyber security challenges for IoT-based smart grid networks. Int J Crit Infrastruct Prot 25:36–49
56. Kłos M, El Fray I (2020) Securing Event Logs with Blockchain for IoT. International Conference on Computer Information Systems and Industrial Management. Springer, Cham, 2020
57. Kosba A et al (2016) Hawk: The blockchain model of cryptography and privacy-preserving smart contracts.“ 2016 IEEE Symposium on Security and Privacy (SP). IEEE
58. Kshetri N (2017) Can blockchain strengthen the internet of things? IT Prof 19(4):68–72
59. Kulkarni O (2019) Preventing the Man-in-the-Middle Attack on Internet Communication using Blockchain Technology. Diss. Dublin, National College of Ireland
60. Kumar G et al (2019) Proof-of-Work consensus approach in Blockchain Technology for Cloud and Fog Computing using Maximization-Factorization Statistics. IEEE Internet Things J
61. Kumar T et al (2020) BlockEdge: Blockchain-Edge Framework for Industrial IoT Networks. IEEE Access 8:154166–154185
62. Kwon D et al (2018) A study on development of the blind spot detection system for the IoT-based smart connected car. 2018 IEEE International Conference on Consumer Electronics (ICCE). IEEE
63. Li F et al (2019) Enhanced Cyber-Physical Security in Internet of Things through Energy Auditing. IEEE Internet Things J
64. Li X et al (2020) A survey on the security of blockchain systems. Future Gener Comput Syst 107:841–853
65. Li M et al (2020) LEChain: A blockchain-based lawful evidence management scheme for digital forensics. Future Gener Comput Syst 115:406–420

66. Li S, Qin T, Min G (2019) Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems. IEEE Trans Comput Soc Syst 6(6):1433–1441
67. Lin J et al (2020) Mcunet: Tiny deep learning on IoT devices. arXiv preprint arXiv:2007.10319
68. Lonzetta AM et al (2018) Security vulnerabilities in Bluetooth technology as used in IoT. J Sens Actuator Netw 7(3):28
69. Luque-Vega, Luis F et al (2020) Smart Cities Oriented Project Planning and Evaluation Methodology Driven by Citizen Perception—IoT Smart Mobility Case. Sustainability 12.17:7088
70. Madhugundu DK, Ahmed F, Roy B (2018) A Survey on Security Issues and Challenges in IoT Based Smart Home. Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT)
71. Malkar N et al (2019) Survey Paper on An IoT Based Smart Parking System
72. Manne JM et al (2020) Smart Automation using IoT. Int J Res Appl Sci Eng Technol (IJRASET) 8(V)
73. Meneghello F et al (2019) IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet Things J
74. Mercan S et al (2020) A Cost-efficient IoT Forensics Framework with Blockchain. arXiv preprint arXiv:2004.14691
75. Mercan S et al (2020) A Cost-efficient IoT Forensics Framework with Blockchain. arXiv preprint arXiv:2004.14691
76. Mishra L, Varma S (2020) Internet of Things for Military Applications. (2020) 7th International Conference on Computing for Sustainable Global Development (INDIACom). IEEE
77. Nadeem K, Saeed N, Ahmed N (2020) A Comparative Study of Digital Forensics and Cybercrime Investigation
78. Nasralla MM, García-Magariño I (2020) and Jaime Lloret. “Defenses Against Perception-Layer Attacks on IoT Smart Furniture for Impaired People. IEEE Access 8:119795–119805
79. Neshenko N et al (2019) Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. IEEE Communications Surveys & Tutorials
80. Nieto A, Rios R, Lopez J (2017) A methodology for privacy-aware iot-forensics. Proc 16th IEEE Int Conf Trust Secur Priv Comput Commun 11th IEEE Int Conf Big Data Sci Eng 14th IEEE Int Conf Embed Softw Syst 626–633
81. Novak M (2020) Digital Evidence in Criminal Cases Before the US Courts of Appeal: Trends and Issues for Consideration. J Digit Forensics Secur Law 14(4):3
82. Olivares-Rojas JC et al (2018) A Comparative Assessment of Blockchains in Embedded Systems. 2018 IEEE International Autumn Meeting on Power, Electronics and Computing (ROPEC). IEEE
83. Pajila PB, Julie EG (2019) Detection of DDoS Attack Using SDN in IoT: A Survey. Intelligent Communication Technologies and Virtual Mobile Networks. Springer, Cham
84. Palmer G (2001) A road map for digital forensic research. First digital forensic research workshop, utica, new york
85. Panwar N et al (2019) “Smart Home Survey on Security and Privacy.“ arXiv preprint arXiv:1904.05476
86. Pawanraj SP, Jagadeesh BN (2020) Design of IoT Robot for Military Applications
87. Pradhan M (2018) “A Survey of Smart City Assets for Future Military Usage.“ 2018 International Symposium on Networks, Computers and Communications (ISNCC). IEEE
88. Praveen MM, Dhandapani S (2020) “IOT Based Military Robot Enhanced With Raspberry PI”. Solid State Technol 63(5):7195–7202
89. Qian LP et al (2019) “HybridIoT: Integration of hierarchical multiple access and computation offloading for IoT-based smart cities”. IEEE Network 33(2):6–13
90. Radhika R, Kulothungan K (2019) Mitigation of Distributed Denial of Service Attacks on the Internet of Things. Appl Math 13(5):831–837
91. Rana MM, Bo R (2020) “IoT-based cyber-physical communication architecture: Challenges and research directions”. IET Cyber Phys Syst Theory Appl 5(1):25–30
92. Restuccia F et al (2019) Blockchain for the Internet of Things: Present and Future. arXiv preprint arXiv:1903.07448
93. Reyna A et al (2018) “On blockchain and its integration with IoT. Challenges and opportunities”. Future Gener Comput Syst 88:173–190
94. Ricci J, Baggili I, Breitinger F (2019) Blockchain-Based Distributed Cloud Storage Digital Forensics: Where’s the Beef? IEEE Secur Privacy 17(1):34–42
95. Robberts C, Toft J (2019) Finding Vulnerabilities in IoT Devices: Ethical Hacking of Electronic Locks

96. Sadique KM, Rahmani R, Johannesson P (2018) Towards Security on Internet of Things: Applications and Challenges in Technology. Proc Comput Sci 141:199–206
97. Saleh F (2019) Blockchain without waste: Proof-of-stake. Available at SSRN 3183935
98. Salim MM, Rathore S, Park JH (2019) Distributed denial of service attacks and its defenses in IoT: a survey. J Supercomput 1–44
99. Servida F, Casey E (2019) IoT forensic challenges and opportunities for digital traces. Digit Investig 28:S22–S29
100. Shaaban A, Konstantin S (2016) Practical Windows Forensics. Packt Publishing Ltd
101. Sharma V et al (2019) Security, Privacy and Trust for Smart Mobile-Internet of Things (M-IoT): A Survey. arXiv preprint arXiv:1903.05362
102. Shi Y et al (2019) Energy Audition based Cyber-Physical Attack Detection System in IoT.
103. Singh P (2020) Blockchain based Security Solutions with IoT Application in Construction Industry. IOP Conference Series: Earth and Environmental Science 614(1). IOP Publishing
104. Singh S, Kumar S, Rathore, Park JH (2020) Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence. Future Gener Comput Syst 110:721–743
105. Sodhro A, Hassan et al (2019) Towards an optimal resource management for IoT based Green and sustainable smart cities. J Clean Prod 220:1167–1179
106. Sokullu R, Akkaş MA (2020) “Unmanned Aerial Vehicle and IoT as Enabling Technologies for 5G: Frameworks, Applications and Challenges. In: " Internet of Things, Smart Computing and Technology: A Roadmap Ahead. Springer, Cham, pp 217–239
107. Spathoulas G et al (2019) Collaborative Blockchain-Based Detection of Distributed Denial of Service Attacks Based on Internet of Things Botnets. Future Internet 11:226 11)
108. Stanislav M, Tod B (2015) Hacking iot: A case study on baby monitor exposures and vulnerabilities. Rapid 7
109. Stoyanova M et al (2020) A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches and Open Issues. IEEE Commun Surv Tutor
110. Suchitra C, Vandana CP (2016) Internet of Things and Security Issues. Int J Comput Sci Mob Comput 5(1):35–41
111. Syed NF et al (2020) Denial of service attack detection through machine learning for the IoT. J Inf Telecommuni 1–22
112. Tama BA et al (2017) A critical review of blockchain and its current applications.“ 2017 International Conference on Electrical Engineering and Science C (ICECOS). IEEE
113. Tewari A, Gupta BB (2020) Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. Future Gener Comput Syst 108:909–920
114. Thibault L et al (2018) Real-Time Air Pollution Exposure and Vehicle Emissions Estimation Using IoT, GNSS Measurements and Web-Based Simulation Models. 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall). IEEE
115. Tseng L et al (2020) Blockchain-based database in an IoT environment: challenges, opportunities, and analysis. Cluster Comput 23(3):2151–2165
116. Vaccari I, Aiello M, Cambiaso E (2020) Slowtt: A slow denial of service against iot networks. Information 11.9:452
117. Valdeolmillos D et al (2019) “Blockchain Technology: A Review of the Current Challenges of Cryptocurrency.“ International Congress on Blockchain and Applications. Springer, Cham
118. Vangala A et al (2020) Smart secure sensing for IoT-based agriculture: Blockchain perspective. IEEE Sens J
119. Vengatesan K et al (2018) Analysis of Mirai Botnet Malware Issues and Its Prediction Methods in Internet of Things.“ International conference on Computer Networks, Big data and IoT. Springer, Cham
120. von Solms B, von Solms R (2018) Cybersecurity and information security–what goes where? Inf Comput Secur 26(1):2–9
121. Wang C et al (2019) A dependable time series analytic framework for cyber-physical systems of iot-based smart grid. ACM Trans Cyber Phys Syst 3(1):7
122. Wang F et al (2020) A Robust IoT-Based Three-Factor Authentication Scheme for Cloud Computing Resistant to Session Key Exposure. Wirel Commun Mob Comput2020
123. Wang Q et al (2020) Blockchain for the IoT and industrial IoT: A review. Internet Things 10:100081
124. Wang Q et al (2020) A Comparative Study of Blockchain Consensus Algorithms. J Phys Conf Ser 1437(1). IOP Publishing
125. Wang C et al (2020) Industrial Cyber-Physical Systems-based Cloud IoT Edge for Federated Heterogeneous Distillation. IEEE Trans Ind Inform

126. Weber RH (2010) Internet of Things – New security and privacy challenges. Comput Law Secur Rev 26(1):23–30
127. Wheelus C, Zhu X (2020) IoT Network Security: Threats, Risks, and a Data-Driven Defense Framework. IoT 1.2:259–285
128. Wood G (2016) Polkadot: Vision for a heterogeneous multi-chain framework. White Pap
129. Worley C et al (2020) Scrybe: A Second-Generation Blockchain Technology with Lightweight Mining for Secure Provenance and Related Applications. In: Blockchain Cybersecurity, Trust and Privacy. Springer, Cham, pp 51–67
130. Xiao Y et al (2019) A Survey of Distributed Consensus Protocols for Blockchain Networks. arXiv preprint arXiv:1904.04098
131. Xiong Y, Du J (2019) Electronic evidence preservation model based on blockchain. Proceedings of the 3rd International Conference on Cryptography, Security and Privacy
132. Xu S et al (2019) A secure IoT cloud storage system with fine-grained access control and decryption key exposure resistance. Future Gener Comput Syst 97:284–294
133. Yang L et al (2018) Hide your hackable smart home from remote attacks: The multipath onion IoT Gateways.“ European Symposium on Research in Computer Security. Springer, Cham
134. Yang F et al (2019) “Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism”. IEEE Access 7:118541–118555
135. Yaqoob I, Hashem IAT, Ahmed A, Kazmi SMA, Hong CS (2019) Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. Futur Gener Comput Syst 92:265–275
136. Yao Y et al (2019) Identifying Privilege Separation Vulnerabilities in IoT Firmware with Symbolic Execution. European Symposium on Research in Computer Security. Springer, Cham
137. Yu Q, Zhang Z, Dofe J (2020) Proactive Defense Against Security Threats on IoT Hardware. Model Des Secur Internet Things 407–433
138. Zaidan AA, Zaidan BB (2020) A review on intelligent process for smart home applications based on IoT: coherent taxonomy, motivation, open challenges, and recommendations. Artif Intell Rev 53(1):141–165
139. Zaidan AA et al (2018) “A survey on communication components for IoT-based technologies in smart homes”. Telecommun Syst 69(1):1–25
140. Zaidi N et al (2018) A Study of Exposure of IoT Devices in India: Using Shodan Search Engine. Information Systems Design and Intelligent Applications. Springer, Singapore, pp 1044–1053
141. Zgheib R et al (2020) “A scalable semantic framework for IoT healthcare applications.“ J Ambient Intell Hum Comput 1–19
142. Zhang S, Lee JH (2019) Double-spending with a Sybil Attack in the Bitcoin Decentralized Network.“ IEEE Trans Ind Inform
143. Zhang S, Lee JH (2020) Analysis of the main consensus protocols of blockchain. ICT Express 6(2):93–97
144. Zheng S et al (2018) User perceptions of smart home IoT privacy. Proceedings of the ACM on Human-Computer Interaction 2.CSCW 200
145. Zhou Z et al (2019) Potential risk of IoT device supporting IR remote control. Comput Netw 148:307–317
146. Zieliski Z, Chudzikiewicz J, Furtak J (2019) An Approach to Integrating Security and Fault Tolerance Mechanisms into the Military IoT. Security and Fault Tolerance in Internet of Things. Springer, Cham, pp 111–128
147. Zyskind G, Nathan O, Pentland A (2015) Enigma: Decentralized computation platform with guaranteed privacy. arXiv preprint arXiv:1506.03471

Randa Kamal Soltan has received her B.Sc. from The Department of Computers and Control, Faculty of Engineering, Tanta University, Tanta, Egypt, in 2001. She received her M.Sc. from The Department of Computers and Control, Faculty of Engineering, Tanta university, Tanta, Egypt, in 2017. She is currently studying for Ph.D. degree in computer science from the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Egypt. She is currently a Head of IT support sector in Telecom Egypt “WE”, Egypt. Her current research interests include Internet of Things (IoT), Blockchain, Digital Forensics, Cyber security.

Ezz El-Din Hemdan has received his B.Sc from the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Egypt, in 2009. He received his M.Sc. From the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Egypt, in 2013. He received his Ph.D. degree in the Department of Computer Science, Mangalore University, India in 2018. He has several publications in national/international conferences and journals. His research area of interest includes; Canacelable Biometric, Blockchain, Digital Twins, Image Processing, Virtualization, Cloud Computing, Internet of Things/Nano-Things, Cryptography, Data Hiding, Digital Forensics, Cloud Forensics, Big Data Forensics, Data Science and Big Data Analytics.

Nawal El-Fishawy received a Ph.D. degree in mobile communications, Faculty of Electronic Eng., Menoufia University, Menouf, Egypt, in collaboration with Southampton University in 1991. Her research interest includes computer communication networks with emphasis on protocol design, traffic modeling, and performance evaluation of broadband networks and multiple access control protocols for wireless communications systems and networks. Now she directed her research interests to the developments of security over wireless communications networks (mobile communications, WLAN, Bluetooth), VOIP, and encryption algorithms. She has served as a reviewer for many national and international journals and conferences.