Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 5579148, 30 pages
https://doi.org/10.1155/2021/5579148

Review Article

Threats and Corrective Measures for IoT Security with Observance of Cybercrime: A Survey

Sita Rani,[1] **Aman Kataria**,[2] **Vishal Sharma**,[3] **Smarajit Ghosh**,[4] **Vinod Karar**,[2] **Kyungroul Lee**,[5] **and Chang Choi**[6]

[1]*Department of Computer Science & Engineering, Gulzar Group of Institutes, Khanna, 141401 Punjab, India*
[2]*Optical Devices and Systems, CSIR-CSIO, Chandigarh 160030, India*
[3]*EEECS, Queen's University Belfast, UK*
[4]*Department of Electrical and Instrumentation Engineering, Thapar Institute of Engineering and Technology, Patiala, India*
[5]*School of Computer Software, Daegu Catholic University, Gyeongsan-si, Republic of Korea*
[6]*Department of Computer Engineering, Gachon University, Seongnam, Republic of Korea*

Correspondence should be addressed to Vishal Sharma; vishal_sharma2012@hotmail.com

Received 5 January 2021; Revised 28 March 2021; Accepted 31 March 2021; Published 28 April 2021

Academic Editor: Dario Bruneo

Internet of Things (IoT) is the utmost assuring framework to facilitate human life with quality and comfort. IoT has contributed significantly to numerous application areas. The stormy expansion of smart devices and their credence for data transfer using wireless mechanics boost their susceptibility to cyberattacks. Consequently, the cybercrime rate is increasing day by day. Hence, the study of IoT security threats and possible corrective measures can benefit researchers in identifying appropriate solutions to deal with various challenges in cybercrime investigation. IoT forensics plays a vital role in cybercrime investigations. This review paper presents an overview of the IoT framework consisting of IoT architecture, protocols, and technologies. Various security issues at each layer and corrective measures are also discussed in detail. This paper also presents the role of IoT forensics in cybercrime investigation in various domains like smart homes, smart cities, automated vehicles, and healthcare. The role of advanced technologies like artificial intelligence, machine learning, cloud computing, edge computing, fog computing, and blockchain technology in cybercrime investigation is also discussed. Lastly, various open research challenges in IoT to assist cybercrime investigation are explained to provide a new direction for further research.

1. Introduction

The term "Internet of Things" (IoT) characterizes the network of devices—"things"—which are equipped with different types of sensors, advanced technologies, and software. Although the concept of IoT was introduced by Kevin Aston in the year 1999, it developed very briskly only in the last few years and has become one of the most prominent technologies of this era [1, 2]. Smart devices and things have the features to gather, process, and communicate data to deliver several services and applications for the convenience of users [3–5]. Consequently, it is not a single technology but a strong merger of 5G and beyond, big data, artificial intelligence, edge computing, FinTech, and cloud computing [6] (as shown in Figure 1, which represents IoT as a conflux of technologies).

In a short period, IoT has been deployed in many domains. Their applications range from simple household devices to very complex and sophisticated industrial equipment and machines. Smart healthcare, supply chains, smart farming, unmanned vehicles, smart homes, underwater IoT sensors, smart cars, smart grids, and smart industries are some of the areas that have benefitted the most from IoT (as shown in Figure 2) [7, 8]. IoT has also transformed a wide range of objects into devices that provide more lifestyle-friendly digitized services [9].

As all the smart devices are connected through cyberspace, an increase in their number has also widened the

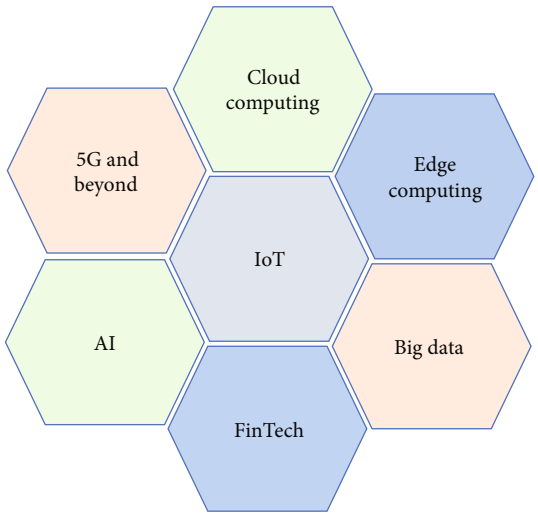

Figure 1: IoT: a conflux of technologies [1, 3, 5, 6].

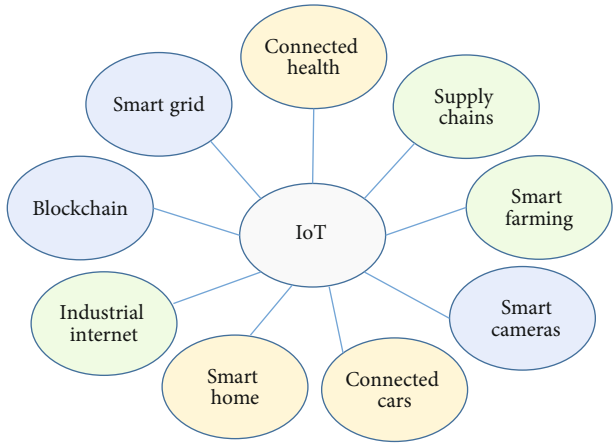

Figure 2: Different applications of IoT [1, 6, 194–199].

attack surface for cybercrime. Although the domain of cybersecurity benefitted from its involvement with IoT devices, it also introduced different types of security issues [10]. A sharp hike is observed in the statistics of security attacks and cybercrimes across the world based on the reports published by the Internet Crime Complaint Centre (IC3) in the year 2019 (as shown in Table 1). From the year 2015 to 2020, a total of 3,919,014 complaints have been received, which caused a total loss of $23.5 billion. Based on the facts published by IC3, India is 3rd in the list of the top 20 countries that were victims of cybercrimes [11].

The era of IoT-enabled devices is blooming expeditiously. This rapid development is introducing both opportunities and obstacles for the identification of physical and cyber threats [12]. These attacks are malignant actions intended to damage significant data and information and to disturb important services [13, 14] in different types of IoT devices equipped with sensors [15]. IoT-enabled devices facilitate the process of cybercrime detection but are themselves prone to cyber threats. One workable security solution lies at the

Table 1: Data on crime complaints and financial losses from 2015 to 2020 [16, 231].

Year	Number of complaints registered	Total loss (in $billion)
2015	288012	1.1
2016	298728	1.5
2017	301580	1.4
2018	351937	2.7
2019	467361	3.5
2020	2211396	13.3

manufacturer's end. At the time of design and development of smart devices and applications, it is necessary to practice secure technologies and protocols. However, IoT-enabled devices provide an increased attack surface for cyber threats due to indigent security measures. Security threats are severely tormenting versatile IoT systems. The level of the security threats in the IoT domain may be even life threatening.

Data from the main academic databases have been collected to study the scope of potential research in the domain of cybersecurity in IoT [16]. Figure 3 depicts the number of research papers referred to in the survey related to security issues in IoT from the year 1998 to 2020. As analyzed, this area of research has gained a lot of importance in the last decade.

Keeping in view the relevance of the domain and the need of the hour, in this paper, we discuss IoT architecture, security systems, and potential IoT security threats that may cause cybercrimes to occur. IoT forensics and its contribution to crime investigation are also discussed in detail. Table 2 presents the merits of this survey in comparison to the latest existing surveys. It visualizes the novelty of this survey as much emphasis is focused on cybercrimes, patents reported, and real-time applications developed to mitigate the problems occurring due to cybercrimes in IoT devices.

In the remainder of this paper, Section 2 is focused on the various types of risks associated with the IoT environment. Existing work on IoT security and cybercrime and the scope of this survey are presented in Section 3. Section 4 is focused on the IoT framework and applications. The role of digital forensics in cybercrime investigation is elaborated in Section 5. Section 6 presents the role of advanced technologies in IoT security. To provide a new direction to researchers, open research challenges in this domain are discussed in Section 7. The paper is then concluded in Section 8.

2. Risks in IoT

The IoT evolution is prone to cause a diversity of ethical problems in society like unauthorized access to confidential information, privacy breach, misuse of secret data, and identity theft. Although these problems were already existing in the era of the internet and Information and Communication Technology (ICT), they have become more dominant in IoT systems [17]. Figure 4 describes several potential risks associated with IoT.

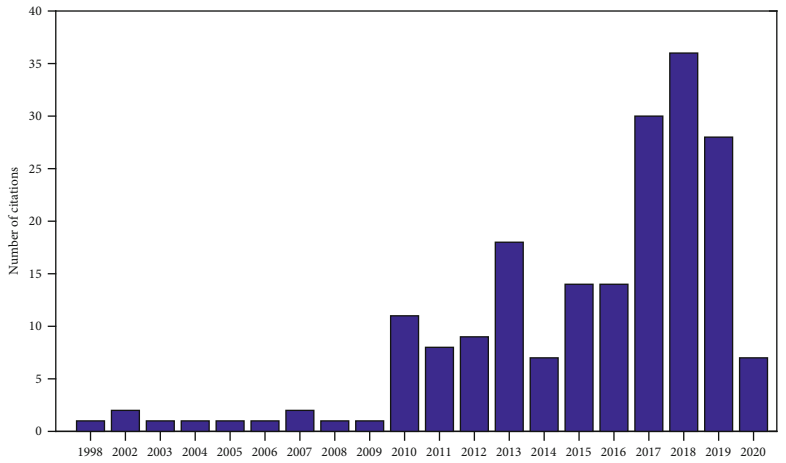

Figure 3: Number of articles cited in this survey from the year 1998 to 2020.

Table 2: Comparison of features of this survey with the existing survey articles.

S. No.	Author	Year	Cyberattacks and security	Cybercrime	Security in IoT devices	Privacy in IoT devices	Patents reported	Discussions on real-time applications
1	Burhan et al.	2018	✗	✗	✓	✓	✗	✗
2	Williams et al.	2018	✓	✓	✗	✗	✗	✗
3	Huang et al.	2018	✓	✓	✗	✗	✗	✗
4	Bhat and Dutta	2019	✓	✗	✓	✗	✗	✓
5	Mrabet et al.	2018	✓	✗	✗	✗	✗	✗
6	Tounsi and Rais	2017	✓	✓	✗	✗	✗	✓
7	Jian-hua Li	2018	✓	✗	✗	✗	✗	✗
8	Khadam et al.	2020	✓	✗	✓	✓	✗	✗
9	Shafiq et al.	2018	✓	✗	✗	✗	✗	✗
10	Weichbroth and Lysik	2020	✓	✓	✓	✗	✗	✗
11	This survey	2021	✓	✓	✓	✓	✓	✓

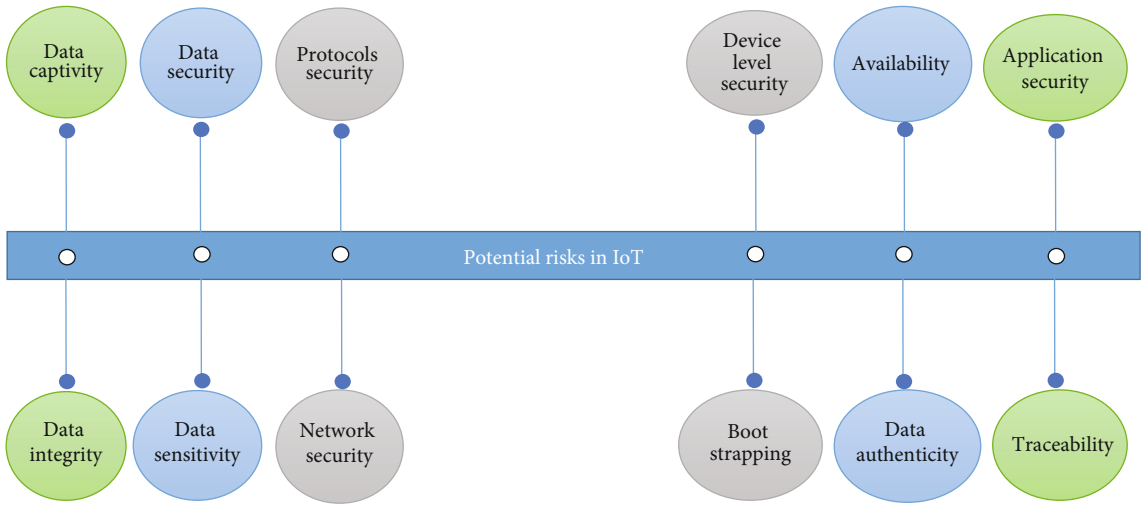

Figure 4: Risks of IoT [17, 132, 170, 200–202].

2.1. Privacy Facet. The confidentiality of users and the secrecy of the data generated from numerous business processes are the major areas of concern linked to the IoT [18]. The dominant usage of versatile devices with poor security mechanisms leads to mismanagement of the IoT system [19]. To handle the security issues related to data generated by the IoT devices, there is a requirement for advanced cryptography techniques. However, these techniques should be energy optimized and have the potential to synchronize with the dynamism of smart devices [20]. With the advancement in IoT, many of the following privacy issues evolved [17] [21]:

(i) Data captivity: a few moralistic questions related to user data remain unanswered, such as generating unlawful leverage and hard competition. These issues are essential to evade consumer captivity through data [22]

(ii) Data integrity: the consistency and accuracy of the data are the primary requirements for the integrity of the data in IoT devices. Maintaining data integrity is the main motive of enterprise security solutions as compromising data integrity can lead to the loss of sensitive data. Data integrity is necessary for reusability, searchability, recovery, and traceability of the data

(iii) Data security: the data must be secured from illegitimate usage on the devices as well as during transmission in the IoT environment. The diversity of the IoT devices and the different communication modes cause a challenge for data security protocols, which is the root cause of security breaches [23]. Another major threat to data security are the various applications using this data which expose the personal information of the user to cyberattacks

(iv) Data sensitivity: several applications collect a user's personal information sometimes even without the user's knowledge. Therefore, the sensitivity of the data is a major area of concern. The major risks associated with this data are the frame of reference of usage of this data. Consequently, there should be some security protocols for context-aware data collection and usage [24]

(v) Protocol security: because of the versatility of devices and collaborators convoluted in the stationing of IoT, the biggest challenge is the applicability of law and regulations for the formation of authentic protocols for communication in the IoT. As the IoT systems are evolving day by day and becoming global, there is also a clear possibility of the applicability of multiple legislations. Besides, this is an important area for awareness among users, IoT manufacturers, and law builders

(vi) Network security: the network plays a vital role in the security of IoT devices. The IoT device is connected to the network for data and workload. This data can become an easy target for hackers or attackers who can compromise the whole system. It is necessary to adapt and devise effective methods to protect the network to which the IoT device is connected

(vii) Device-level security: the security of an IoT device is considered at the beginning of its design. To ensure the secure implementation of an IoT device, a secure architecture is deployed. During the manufacturing of an IoT device, care is taken in terms of secure digital device IDs. The credentials used should be those that can be trusted to tackle various attacks like data and device cloning, data tampering, or any other misuse

(viii) Boot strapping: bootstrapping refers to any process which occurs before any IoT device becomes operational. Bootstrapping is necessary for the IoT devices of the present generation. The time of bootstrapping in the initial configuration of an IoT device plays a vital role. Therefore, the bootstrapping process in IoT devices should be a highly secure process

(ix) Availability: the blending of IoT in services related to health, security, etc. has made the continuous availability of these services a critical issue. Many people are heavily dependent on the IoT devices utilized to provide these services. Therefore, any loss to these services will severely impact human life

(x) Data authenticity: ownership of the collected user data is a major unaddressed issue in IoT along with data management. Once the user stops using the service, the personal information remains with the service provider and can be sold to generate revenue

(xi) Application security: the applications designed for various IoT devices are also vulnerable to different types of attacks. It is necessary that the application should be secure and defensive in nature to counterattack the attackers and malwares. There are different types of attacks which can intrude in the architecture of an IoT device like DDoS, spam attack, message interception through a spyware, a vulnerable 3pp library, and injection attacks

(xii) Traceability: in an IoT environment, users must have the right to pass consent to provide personal information to numerous real-life services. The implemented security protocols and mechanisms should ensure user identification on the network, but restrict the user traceability to attackers from personal information [25, 26]

2.2. Security Facet. The security of a computer system encompasses various methods and techniques that safeguard all kinds of resources from illegitimate access. Resources may include hardware, software, and data, whereas illegitimate

access may include unauthorized usage or damage to resources. In IoT systems, security aspects focus on architecture, the security model of every device, bootstrapping, network security, and application security [27]. Security architecture demonstrates the various system components involved in ensuring the security of an IoT device. The security model of each device focuses on the implementation of security methods and criteria along with the management of various applications. Network security deals with the reliable functioning of IoT. Online application security is all about the authentication of various things on the network for communication and exchange of data. Network security is highly dependent on the internet, which is an anxious media of data exchange and leads to a large possibility of data stealing. The deployment of IoT is dependent on the internet and computer networks. Consequently, it is affected by all security issues related to computer networks as well as the internet. Before using IoT devices, all stakeholders should analyze the associated risks related to the security and privacy of the user information. Accordingly, more sophisticated security policies must be designed by governing organizations.

2.3. Cybercrime. Like any other crime, cybercrime may have a variety of aspects and may be committed in different plots. Several definitions of cybercrime are available, given from different aspects, i.e., sufferers, protector, or viewer. According to the definition given by Marion [28], cybercrime is an action in which computers or computer networks are used as a means, purpose, or platform to execute some criminal act. It may consist of some information theft or usage of computers to do some other criminal activity. The Council of Europe's Cybercrime Treaty defines cybercrime as any act of data content or copyright transgression. The "Manual on the Prevention and Control of Computer-Related Crime" by the United Nations defines cybercrime as illegitimate access, deceit, and falsification. According to Gordon and Ford, cybercrime is any criminal activity performed on a computer, hardware resource, or network. The Council of Europe's Convention on Cybercrime classifies criminal acts into four classes: (1) breaches of data, secrecy, integrity, and hardware resources; (2) computer-centered crimes; (3) content-related crimes; and (4) copyright-related crimes. However, these classifications are over the line for some parameters. According to another classification given by Saini et al. [29], cybercrimes are categorized as data crimes, network crimes, access crimes, and content-related crimes. Data crimes consist of data stealing, data interception, and data modification. Network crimes include unwanted interference in the functioning of computer networks to breach data transmitted over the network. Content-related crimes include infringement of ownership and spontaneous cyber hazards. Another explanation of cybercrime is demonstrated by Zhang et al. [30]; according to them, all crimes in which machines or networks are used as aids, targets, or the place of crime and any conventional crime executed with computer resources are considered cybercrime. Generally, ICT boosts the rate as well as the domain of criminal actions. The location of crime acts as a catalyst for criminal activities [31]. Internet is also a large platform for criminal acts as it was not initially deployed with highly secure protocols. As IoT systems are implemented on the ceiling of the present internet framework, the associated cybercrime issues remain unresolved. Lastly, the large base of the cyber framework enhances the inclination not to reveal these criminal acts to the public as the criminal acts are executed using virtual methods.

3. Existing Work on IoT Security and Cybercrime

In the last few years, several surveys have been conducted to impress upon the improvements and research carried out in the IoT systems. In these survey papers, the focus is on the fundamental aspects of IoT. Along with IoT, security issues are also discussed in some of these surveys. There are few dedicated survey papers on IoT security and privacy contention. In the surveys published in the years 2010-2020, Atzori et al. [32] discussed the security and privacy aspects of IoT. In the field of security, the main attention is given to authentication and data integrity, and the scope of research is discussed. In the privacy aspect, the authors suggested limiting access to personal data. However, this survey highlights incomplete facts regarding security challenges in IoT. Miorandi et al. [33] assumed the implementation of IoT at three fundamental levels, i.e., communication, identification, and interaction. The authors highlighted the possibility of many security challenges in IoT but proposed research on three main issues: the privacy of users, data secrecy, and trust. Many burning issues related to IoT security like access control, data integrity, and authentication of the user are not discussed in detail [34]. Gubbi et al. [35] discussed security and privacy in the contexts of user identification and authentication, data integrity, and privacy in general. The authors introduced the cloud-based IoT paradigm. On the same grounds, few technologies are introduced along with the domains of application of each technology.

In [36], Aggarwal et al. discussed a security prospectus exclusively from a privacy perspective, whereas other security challenges in IoT platforms are not discussed. Said [37] discussed various IoT architectures along with research issues. In this survey, only challenges faced in physical security and privacy are explored. Moreover, security issues are discussed without giving any viable solutions. Perera et al. [38] elaborated that security and privacy challenges are handled at the middleware level in the IoT framework and at different layers. In this survey, security is expressed as a normal issue and the authors did not pay any special attention to the research in the field. Granjal et al. [39] presented an in-depth review of the different security mechanisms and protocols of the time for communication among smart devices. The authors also highlighted the available scope of research. However, on the negative side, the authors did not consider all security standards in their survey but focused on only a few. Sicari et al. [40] reviewed security from three different angles: security requirements, privacy, and trust. Under security requirements, the authors explored the issues related to access control, confidentiality, and authentication. The

biggest drawback of this work is the inadequacy of the categorization of research activities in the IoT security paradigm. Abomhara and Køein [41] reviewed the security threats along with the security and privacy research challenges in their paper. They stressed research issues like interoperability of diverse IoT devices and authorization.

Mahmoud et al. [42] surveyed IoT security principles. The authors also presented various security issues along with corrective measures. The need for advanced technologies to tackle hardware, software, user identification, and wireless communication issues is also discussed. Pescatore and Shpantzer [43] presented the viewpoint of people actively involved in the research of IoT security issues along with the future prospects in the field. They also highlighted that IoT developers should focus more on security issues instead of other ICT systems. Gil et al. [44] reviewed various technologies and security models in the context of data-related challenges. The authors impressed upon the collaboration of social networks and IoT and introduced a new concept of the Social Internet of Things (SIoT). IoT security is discussed but the concept of cybersecurity in IoT is not touched. Muhammad et al. [45] discussed the various possible attacks in IoT systems. The authors also highlighted the security and privacy challenges faced in the IoT environment by the various sensor nodes. In this survey, the requirements of secure end-to-end communication among smart devices using efficient encryption and authentication methods are suggested. Vignesh and Samydurai [46] reviewed the three-layered architecture of IoT comprised of the application, network, and perception layers, along with the different types of security threats at these layers. They explained the effect of wireless signals, movement of IoT in the external environment, and the dynamism of the network model as the major challenges at the perception layer. At the network layer, the major highlighted challenges are DoS and Man-in-the-Middle attacks. The major issue that persists at the application layer is the variety of application policies.

Razzaq et al. [47] surveyed the different security requirements of an IoT system. The authors categorized the various IoT attacks into four classes: low level, medium level, high level, and extremely high level. They also suggested the possible ways out in handling these attacks. Maple [48] discussed the role of IoT devices in various domains like autonomous vehicles, health, industry 4.0, logistics, smart grid, agriculture, homes, offices, and entertainment. Along with the security, threats in all these application areas are also reviewed. They highlighted the security issues related to the physical limitations of the things, the versatility of the devices, authentication, authorization, and implementation. Various issues related to the privacy of the users are also discussed in this survey. Rughani [49] presented the various challenges faced by crime investigators to collect pieces of evidence from the smart IoT devices available at crime scenes. The author impressed upon the need for corrective measures for the issues to help in crime investigation and make the process easy. Corser et al. [50] discussed that to make the IoT systems more secure, the security of smart devices and networks needs to be improved. To improve device-level security, protection of data and dynamic testing play a major role. To make communication networks more reliable, there is a requirement for authentication, secure protocols, network division, and organization. Burhan et al. [51] presented a detailed survey on the different layers of the IoT architecture along with the potential attacks at each layer. The authors also reviewed various available mechanisms to handle these attacks and their limitations. Security issues in various IoT technologies like sensors, ZigBee, Bluetooth, RFID, Wi-Fi, and 5G networks are discussed in detail.

Noor and Hassan [52] presented the primary objectives of IoT system security. The authors highlighted that the privacy of the user and the security of the data and infrastructure are the main challenges in the IoT environment. The authors also reviewed various tools and simulators to implement IoT security mechanisms. MacDermott et al. [53] highlighted the sharp increase in the usage of digital forensics for crime investigation. The authors also highlighted that the reason for this rise is the increase in smart devices. To cope up with this change, there is a need for regular development in the techniques used for crime investigation. The authors also reviewed various forensic handling methodologies. Riahi Sfar et al. [54] presented three different aspects, i.e., privacy, trust and identification/authentication of IoT security. Under these three aspects, various open research issues like standardization of security mechanisms, reduction in the amount of data transmitted among smart devices, implementation of trust mechanisms to safeguard users and services, implementation of a global identification mechanism for things, and automatic discovery of devices in the IoT environment are highlighted.

Neshenko et al. [55] presented an exhaustive survey on IoT vulnerabilities. The need for the endorsement of different advanced technologies like blockchain, deep learning, and cloud paradigms is stressed in IoT security implementation. Various research aspects highlighted in the survey are the requirement of global device identification mechanisms, the need for more security-centric awareness among IoT users, the requirement of more mature security protocols, and the adoption of secure IoT application development processes. Zhou et al. [56] reviewed four main features of IoT: interdependence, diversity, constraint, and myriad. Consequently, the open research issues for these have also been discussed. It is spotlighted in the survey that in IoT systems, the devices are interdependent, so focusing on security mechanisms by considering each device as a standalone will not provide a secure IoT environment. Detection of viruses in IoT devices is also highlighted as an open research challenge in this survey. The issue of sensitivity of the user's personal information is also an area of major concern for academicians and researchers. Lu and Xu [11] elaborated that the privacy and security of IoT systems is the biggest research challenge. The authors presented a detailed review of the state-of-art research going on in cybersecurity. IoT architecture for cybersecurity is discussed in detail. Lastly, the major research challenges of the domain are also presented. Aydos et al. [57] classified IoT vulnerabilities depending upon the types of attack in four different layers: physical layer, network layer, data processing layer, and application layer. Depending on these vulnerabilities, the authors proposed a risk-based

security model to evaluate each discussed layer of the IoT architecture. Nasiri et al. [58] surveyed the security needs of an IoT-dependent health care system. They classified it into two categories: cybersecurity and cyber resilience. Under cybersecurity, the various features of confidentiality, integrity, availability, identification, authentication, authorization, privacy, accountability, nonrepudiation, auditing, and data freshness are elaborated. Under cyber resilience, safety, survival, performance, reliability, maintenance, and information security are discussed in detail. Tabassum et al. [59] reviewed various IoT security challenges. The authors also demonstrated the role of IoT in industry. This study presented how the security issues of individual devices/things used at each layer in the IoT architecture can affect the security of an IoT system.

Servida and Casey [12] presented a detailed study of the vulnerabilities of smart devices. The authors discussed how these vulnerabilities can cause these devices to become victims of attacks. On the positive side, it is featured that these vulnerabilities can help the investigators capture digital traces and investigate the crime. Therefore, device vulnerabilities are both challenges and opportunities in crime. Blythe et al. [60] highlighted that the IoT environment lacks security features as the devices are not manufactured with security challenges taken into consideration. It is also discussed that at some events, even users do not use the available security features of the devices due to a lack of knowledge about the customization of these features. In this work, the authors impressed on the need for the standardization of communication and security protocols in IoT systems and highlighted the need for government intervention to assure security at the device level. Adesola et al. [61] suggested a novel IoT and big data-based smart model to investigate and control criminal activities in Nigeria. The authors also developed a prototype for the model. This model is useful to keep records of criminals. Abdullah et al. [16] discussed the security aspects of IoT by focusing on cybersecurity. Open research issues related to cybersecurity are highlighted along with possible corrective measures. The authors also applied the usage of blockchain technology to strengthen the cybersecurity aspect of IoT. Butun et al. [1] presented an in-depth review of various types of security attacks in wireless sensor networks and IoT systems. Various mechanisms for the prevention and detection of these attacks are also discussed in detail. The authors categorized the IoT attacks as active and passive attacks. It is also spotlighted that passive attacks cannot be identified using any mechanism. On the other hand, active attacks violate the integrity and confidentiality of data. Active attacks also cause unauthorized access to user data.

Stoyanova et al. [62] surveyed the various available models for digital forensics. Special consideration is given to the methods which are used to extract digital data by maintaining the privacy of the users. The authors presented open research challenges in the field of digital forensics by paying special attention to the need for more advanced forensic analyzing techniques and universally acceptable protocols. Tawalbeh et al. [63] discussed the various security and privacy challenges of IoT. The authors also proposed and evaluated a cloud-based IoT security solution. Atlam et al. [64] reviewed IoT architecture and communication technologies. Various IoT security challenges and threats are also discussed. The authors also explained the role of digital forensics in crime investigation. The need for employing real-time techniques in IoT forensics is highlighted as the need of the hour. Al-Khater et al. [65] presented a detailed review of various categories of cybercrimes in detail. Various cybercrime detection techniques using statistical methods, neural networks, machine learning, deep learning, fuzzy logic, data mining, computer vision, biometrics, and forensics are also discussed. The authors proposed the requirement of cybercriminal profiling, which can be used as a data set by the investigators in the process of investigation. Table 3 presents the comparison of existing security parameters and approaches in IoT cybercrimes.

In this review, we examine the various aspects of IoT systems like architecture, protocols and technologies deployed at various layers and application domains. Potential risks and possible attacks on each layer of the IoT architecture are also discussed. We also present the various security mechanisms and their layers of implementation. Special attention is given to IoT forensics in cybercrime investigations [66, 67]. Various domains like smart homes, smart cities, automated transport, drones, and healthcare are examined to assist cybercrime investigation [68]. The role of various advanced technologies in the investigation of cybercrime is also presented. At the end of the paper, various open research challenges in an IoT environment that contribute towards the process of IoT forensic to aid the process of cybercrime investigation are presented.

4. IoT Framework and Applications

IoT is a broad network of devices connected over the internet. It has expanded very briskly in the last few years. Currently, IoT has evolved as a contemporary styled network that acts as an agent to link the real and virtual world. Application domains of IoT are expanding day by day growing from the need for smartphones to the need for different IoT devices like cameras, music players, smart watches, smart TVs, and smart VRs (as shown in Figure 5). So is the probability of cyberattacks. The fundamental characteristic of IoT applications is to gather data from smart devices and communicate over networks [69]. A gigantic volume of personalized data is gathered by various IoT applications including smart agriculture, healthcare, smart homes, and meetings [70]. This large amount of data is communicated in IoT systems and then interpreted and analyzed. In the research carried out by Cisco, it is estimated that 50 billion smart devices will be plugged into the internet in the current year. It is also predicted that because of their advanced features, smart devices will become an important part of day-to-day life in the current year [57]. It is being foreseen that the trend of using IoT systems will spike and will keep growing afterward. Due to the vast usage of IoT collected data, a new trend has started. Even data collected on smart devices in an IoT environment can be shared for usage in other real-life applications. However, the biggest

Table 3: Comparison of existing security parameters/approaches/models in IoT cybercrime.

Author (year)	Ideology	Parameters	Advantages	Security issues discussed
Atzori et al. (2010) [32]	A survey of internet of things (IoT).	Applications, service management, logistics.	Applications of IoT were discussed in a detailed manner.	✗
Miorandi et al. (2012) [33]	A survey of applications and issues of security in IoT.	Applications, security issues of IoT, research challenges.	Research challenges and issues of securities were explained in detail.	✓
Gubbi et al. (2013) [35]	Application and cloud computing-oriented survey of IoT.	Applications, addressing schemes, cloud computing.	Cloud computing and its applications in IoT were discussed.	✓
Aggarwal et al. (2013) [36]	A survey of applications, data management, and research challenges in IoT.	Applications, data management and analytics, security, privacy.	Data management in IoT and applications were discussed in detail.	✓
Said (2013) [37]	Evaluation of different IoT architectures is presented.	Hierarchical architecture, distributed architecture.	Different IoT architectures were discussed in detail.	✗
Perera et al. (2013) [38]	The authors presented context-aware computing for IoT devices.	Context reasoning, context modelling, context distribution.	Different contexts related to the IoT were presented.	✗
Granja let al. (2015) [39]	Communication protocols and security parameters are discussed in detail.	Different protocols of IoT communications, application layer, physical layer, and MAC layer security.	The security of different layers in IoT communications was discussed in detail.	✓
Sicari et al. (2015) [40]	Research challenges and existing solutions in IoT security are presented in the survey.	Mobile security in IoT, Trust, and privacy in IoT, enforcement in IoT, authentication, confidentiality, and access control in IoT.	Security of IoT was discussed referring to ongoing projects on securing the IoT.	✓
Abomhara and Køein (2015) [41]	Research directions concerning IoT security and privacy are presented.	Different cyberattacks in IoT, security and privacy challenges in IoT, security threats and challenges.	Threats to IoT security were discussed in detail.	✓
Mahmoud et al. (2015) [42]	IoT layer architecture and security features are the key aspects of this paper.	IoT architecture, IoT security issues, IoT security countermeasures.	Basic architectures of IoT and security issues were discussed in detail.	✓
Pescatore and Shpantzer (2016) [43]	Surveyed perceptions on IoT, IoT applications, and industry representation by IoT.	Applications, threats to IoT, risk management in IoT, data monitoring.	The survey conducted with participants was discussed concerning different parameters related to IoT.	✓
Gil et al. (2016) [44]	A general survey of IoT and context awareness of IoT.	IoT applications domain, services for IoT, data mining for IoT.	Services and data as services were discussed. Applications of IoT are also presented.	✗
Iqbal et al. (2017) [232]	A review of security solutions against threats on IoT devices.	Different techniques of attacks on IoT, security and privacy requirements, security solutions in IoT.	The threats to IoT security and its measures to counter the threats were explained in detail.	✓
Vignesh and Samydurai (2017) [46]	A survey on IoT layer architecture and security threats on each layer.	Security features of IoT, architecture, security remedies.	Security issues in IoT and future directions regarding 5G were discussed in the paper.	✓
Razzaq et al. (2017) [47]	A survey on different types of threats in IoT and their solutions is discussed.	Applications of IoT, Threats to IoT, analysis of different types of attacks.	Applications of IoT and analysis of different types of security threats were done.	✓
Maple (2017) [48]	A survey of applications of IoT, authentication, and identity management of IoT, security issues of IoT in different applications.	Applications of IoT in automobiles, health, industry 4.0, agriculture, entertainment, and media.	Security issues on various applications like health and in automobiles were discussed along with privacy challenges in detail.	✓
Rughani (2017) [49]	The authors discussed the architecture of IoT devices along with the security aspects and their application in forensics.	IoT architecture, IoT security issues, and digital security in IoT.	Discussions on forensics in IoT and security issues were discussed.	✓

Table 3: Continued.

Author (year)	Ideology	Parameters	Advantages	Security issues discussed
Corser et al. (2017) [50]	The authors laid prime emphasis on the security of IoT devices.	IoT hardware security, dynamic testing, securing IoT networks.	Certain security issues from a hardware and software perspective were discussed in detail.	✓
Burhan et al. (2018) [51]	Compared the different application domains of IoT and discussed the key elements of IoT.	Applications of IoT, different architecture layers of IoT.	Identity management framework, security mechanisms for IoT, and improved layered architecture for IoT were discussed.	✓
Noor and Hassan (2018) [52]	A survey on IoT security, possible attacks on IoT architecture layers are presented.	IoT security attacks on layer review on IoT authentication, trust management, and secure routing.	Attacks on the IoT architecture layer were explained in detail. Secure routing was presented with key features.	✓
MacDermott et al. (2018) [53]	The authors discussed the IoT, the possible crime using, or in IoT devices.	Forensic handling regarding IoT and crime using IoT devices.	Forensic evidence handling in the smart city was discussed in detail.	✗
Riahi Sfar et al. (2018) [54]	A survey on IoT security including discussion on smart manufacturing.	A cognitive approach for IoT, recent research in data privacy trust management system.	Cognitive and systemic security along with adaptive and context-aware security was discussed in detail.	✓
Neshenko et al. (2018) [55]	A survey on the exploitation of different IoT devices.	IoT architecture security in IoT, IoT vulnerabilities at different architectural layers.	The security aspects of the layer-wise architecture of IoT devices were discussed in detail.	✓
Zhou et al. (2018) [56]	A survey on security features and privacy in IoT.	Attacks on IoT, threats, and challenges in IoT devices.	Threats to IoT hardware devices were discussed in detail.	✓
Lu and Xu (2018) [11]	A survey article on IoT cyberattacks and security schemes.	Different cyberattack and layer-wise security schemes.	Security schemes for different layered architectures were explained in detail.	✓
Aydos et al. (2019) [57]	A survey of risk and threat assessment on different architecture layers of IoT.	IoT applications, platforms for IoT, IoT protocols, security, threats, and vulnerabilities in IoT.	Attack on a different layer in IoT was presented along with a risk-based layered approach for IoT security assessment in detail.	✓
Nasiri et al. (2019) [58]	An article on healthcare-based secure IoT environment.	Security requirements in IoT.	Cybersecurity requirements were discussed.	✗
Tabassum et al. (2019) [59]	An article on various security issues in IoT.	IoT security requirements and architecture of IoT.	Security issues on perception, application, and network layer were discussed in detail.	✓
Servida and Casey (2019) [12]	An article on IoT forensics and detection of traces in IoT.	Digital forensics, privacy, and IoT forensics.	IoT forensics and detection, extraction, and parsing of traces from IoT devices were discussed in detail.	✗
Blythe et al. (2019) [60]	An article on cyber hygiene advice for IoT devices.	Security features of IoT devices, design code of practice for IoT devices.	Standardization of security protocols was the main emphasis.	✓
Adesola et al. (2019) [61]	An article on crime management with IoT-based architecture.	IoT architecture, data collection, and framework for IoT devices.	A crime prediction and monitoring model was proposed.	✗
Abdullah et al. (2019) [16]	A review of cybersecurity issues and challenges.	Cyberattacks, cybersecurity, IoT architecture, and security techniques.	Security techniques at different layers are discussed in detail. The blockchain is implemented to secure the IoT network.	✓
Butun et al. (2019) [1]	A survey on different kinds of attacks and their countermeasures in IoT devices.	IoT applications, security attacks on IoT devices, attacks on different layers of IoT architecture.	Defence against different passive and active attacks on different layers of IoT architecture was discussed in detail.	✓

Table 3: Continued.

Author (year)	Ideology	Parameters	Advantages	Security issues discussed
Stoyanova et al. (2020) [62]	A survey on IoT forensics and its challenges.	IoT forensic components, IoT attacks, IoT security, IoT protocols, IoT layered architecture.	IoT forensics challenges and their solution, secure cloud service models were discussed in detail.	✓
Tawalbeh et al. (2020) [63]	An article on security and privacy in IoT devices.	Generic IoT layers and proposed system model for secure IoT devices.	A system model was proposed using the cloud edge nodes and IoT nodes.	✓
Atlam et al. (2020) [64]	An article on cybercrime, security, and digital forensics for IoT devices.	IoT applications, IoT architecture, characteristics, and communication technologies in IoT, security threats in IoT.	The security solution of four-layered IoT architecture was discussed in detail.	✓

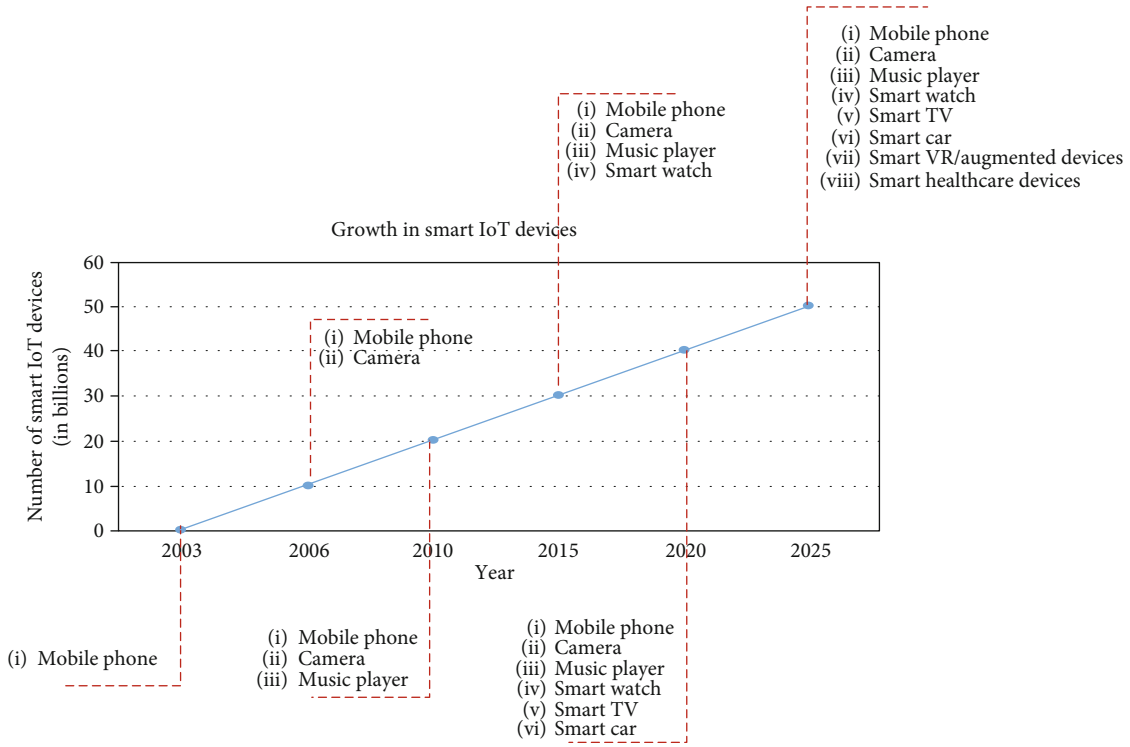

Figure 5: Growth expectations in the type of IoT devices [57, 203–208].

challenge in the collected data is the versatility of smart devices supported in the IoT system architecture.

4.1. IoT Architecture. There is a need for an open architecture to deploy IoT systems to support diverse categories of smart devices and to administer interfacing among them. Many reviews and research articles are available demonstrating this IoT architecture [41]. Fundamentally, IoT systems are deployed on a four-layer architecture as shown in Figure 6. These four layers are the application layer, network layer, perception layer, and transport layer. This is the basic IoT architecture model which can be practiced with different IoT applications. For each layer of the IoT architecture, the possible attacks and the affected domain due to the attack are shown in Figure 6. These technologies help in the process of data collection, interpretation, analysis, and communication [71]. The different layers of the IoT architecture are characterized as follows:

(i) Perception layer: in this layer, data are generated by various smart devices. Data is also gathered by these devices, which can be further communicated within the IoT environment or even to outside applications. This layer works with two types of things: IoT devices and IoT hub nodes [72]. IoT devices identify themselves in the IoT system, whereas IoT hub nodes work as gateways. The data collected through devices are transmitted through gateways [73]

(ii) Network layer: in this layer, communication among IoT devices and applications is managed. The mode

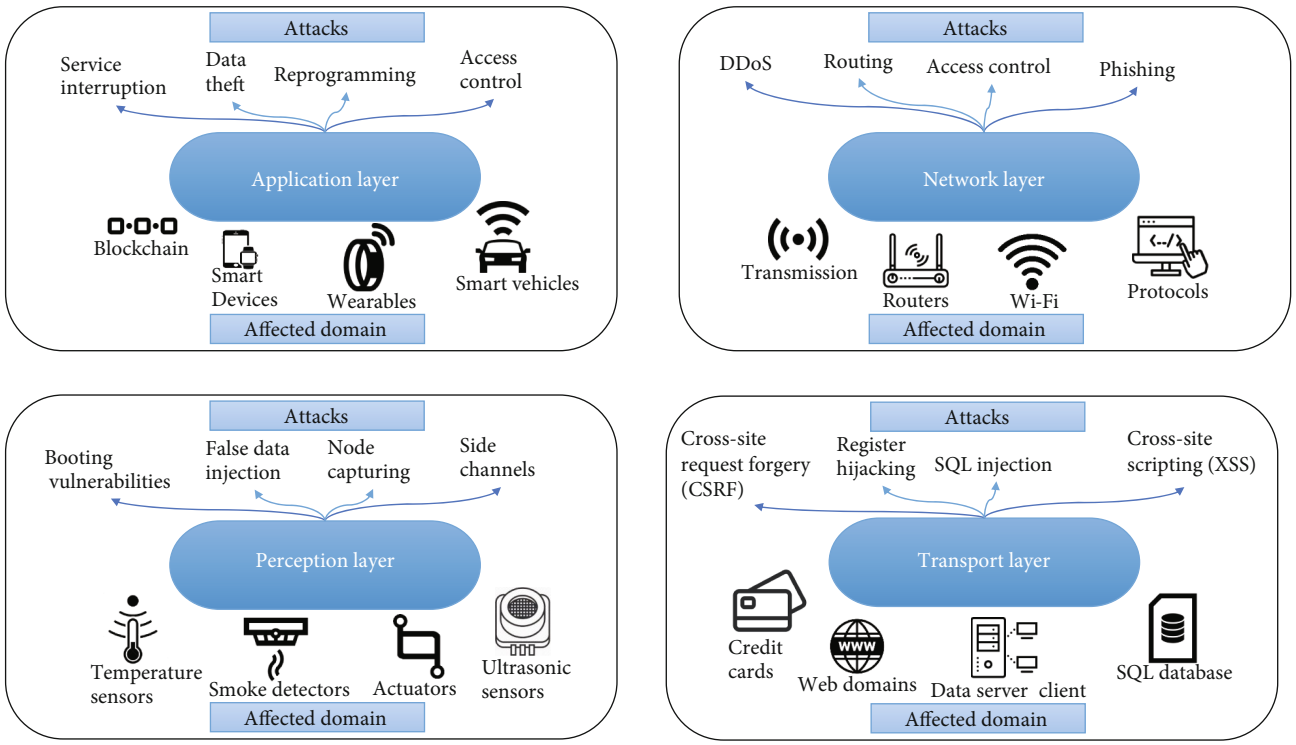

Figure 6: Layers of IoT with technologies deployed and possible attacks [170, 209–214].

of communication may be wired or wireless. Various network security protocols are deployed in the network layer. The IoT gateways are set up at this layer. This layer receives the data coming from the lower layer and maps to the format required by the applications running in the upper layer [74]

(iii) Application layer: the application layer is also interpreted as the service layer. Here, the data gathered by various devices are used, analyzed, interpreted, and presented. This layer can be customized under different policies depending upon the service administered [75]

(iv) Transport layer: the transport layer is responsible for end-to-end communication over the network. It also provides reliability multiplexing along with flow control. Congestion control is also performed in the transport layer [76]

4.2. Protocols. Functionalities provided by the various layers of the IoT architecture are administered by the different protocols deployed in the different layers [77]. The various protocols used at the different layers of the IoT architecture like the application layer, perception layer, network layer, and transport layer are shown in Figure 7. Various protocols deployed in the perception layer are the IEEE 802.11 series, the 802.15 series, Wireless HART (Highway Addressable Remote Transducer), etc. [75]. The IEEE 802.15.4 is used for data exchange in a long-range wireless personal area network (LR-WPAN). ZigBee and Wireless HARTs are also deployed in the IoT perception layer [78].

The protocols used in the network layer of the IoT architecture are IPv6/IPv4, 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks), and 6TiSCH (Time-Slotted Channel Hopping) developed by IETF which is an IPv6 standard for the 802.15.4 MAC layer protocols [79]. IPv6 G.9959 is an IPv6 addressing standard for the G.9959 MAC layer protocol which was designed for low-power devices in a personal area network (PAN). For real-time systems, the Data Distribution Service (DDS) is used. This protocol does not require any networking middleware and network programming, which allow the publisher to release specific information. The lightweight messaging protocol used in the application layer is MQTT (Message Queuing Telemetry Transport), and it uses machine-to-machine communication based on TCP-IP. The protocols specially designed for IoT environments, e.g., CoAP (Constrained Application Protocol) are used in the application layer for limited hardware. The hardware that does not support HTTP can use the CoAP protocol. The XML-based protocol used in the application layer is known as the Extensible Messaging and Presence Protocol (XMPP). XMPP is used for real-time instant messaging and multiparty chat. Simple or Streaming Text Oriented Messaging Protocol (STOMP) is a protocol for message-oriented middleware. It was designed to establish communication between clients and brokers [80–85]. In the transport layer, Datagram Transport Layer Security (DTLS) is designed to prevent message forgery and tampering. The protocol similar to the time-division multiplexing in the transport layer is the Time Synchronized Mesh Protocol (TSMP). It was developed for intersensor communication in timeslots. The message-oriented transport layer protocol is the Stream Control Transmission Protocol (SCTP), which

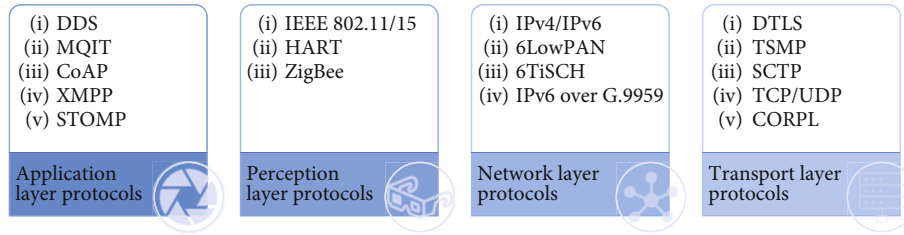

Figure 7: Protocols of different layers in IoT [71, 79, 101, 215].

uses congestion control to transfer data over a network. For large packets and data, the Transmission Control Protocol (TCP) is used in the transport layer in IoT. The User Datagram Protocol (UDP) is a protocol for lesser data; it is used to send data to the server and is suitable for wireless sensor network communication. The extension of the IPv6 routing protocol is Cognitive RPL (CORPL), which was developed especially for cognitive networks. It consists of multiple forwarders with the best node selected to forward the data [86–89].

4.3. IoT Application Domains. The incorporation of smart devices to gather data from our day-to-day life activities make many IoT applications feasible [41]. These applications can be categorized into different domains, summarized as follows:

(i) Personal and social domain: the applications under this domain allow potential users to communicate with the environment or with other users to establish and maintain a social circle [32]

(ii) Mobility and transportation domain: applications falling under this domain include roads and vehicles equipped with sensors and other smart technologies which can gather traffic-related data. This data can help with traffic control and management [90]. Some of the IoT-based transport applications with outstanding performance are the Intelligent Traffic Information Service (ITIS) and the Traffic Information Grid (TIG) [91]

(iii) Enterprise and industrial domain: IoT applications falling under this category include smart banking, manufacturing, logistics, and industrial operations [2, 92]

(iv) Service and utility monitoring domain: this domain of IoT applications commonly deals with smart agriculture, environment, energy management, etc.

4.4. Supporting Technologies. For all applications falling in various IoT domains, different components of the IoT system need to stay connected at all times. This is possible only with IoT supporting technologies [41]. The progressive growth of various technologies like sensors, smartphones, and software will facilitate different things in the IoT systems to stay connected everywhere and at all times [93]. The fundamental approach to support IoT is to connect the objects in the physical world with the digital world [94]. Numerous technologies and devices for these approaches are discussed as follows:

(i) Identification technologies: the fundamental identification technologies used in IoT are Radio-Frequency Identification (RFID) and Wireless Sensor Networks (WSN). These are used in the perception layer of the IoT architecture [19, 32, 92]

(ii) Network and communication technologies: both wired and wireless technologies (e.g., GSM, UMTS, Wi-Fi, Bluetooth, and ZigBee) permit a large number of smart devices and services to be connected [95–97]. A flexible and secure IoT architecture is required for reliable communication among various wireless devices [90]

(iii) Hardware and software technologies: a lot of research is going on in the field of nanoelectronics to develop wide-function and economical wireless IoT systems [92]. Smart things with improved internode communication will help in the development of smart systems assisting fast application development to support various services in IoT

4.5. Security Challenges. Every layer of IoT is prone to security attacks and threats. These attacks may fall under any of the categories of active or passive and internal or external attacks [41, 42]. In passive IoT attacks, only the information transmitted on the network is observed, but the service is not affected. On the other hand, in active attacks, a service stops responding [98]. The various devices and services supported by each layer of IoT are prone to Denial of Service (DoS) attacks. Under DoS attacks, devices, services, and networks become unsalable to unauthorized users. In the same manner, Figure 8 describes the security threats faced by the perception layer, network layer, application layer, and transport layer and services supported at each layer which are discussed as follows:

(i) Security threats in the perception layer: the very first issue faced by the various device nodes functioning in this layer is the intensity of the wireless signals as the signals become weaker due to environmental disturbances. The second issue is related to the physical attacks on the IoT devices as the various IoT nodes usually operate in the outdoor environment. The third issue is related

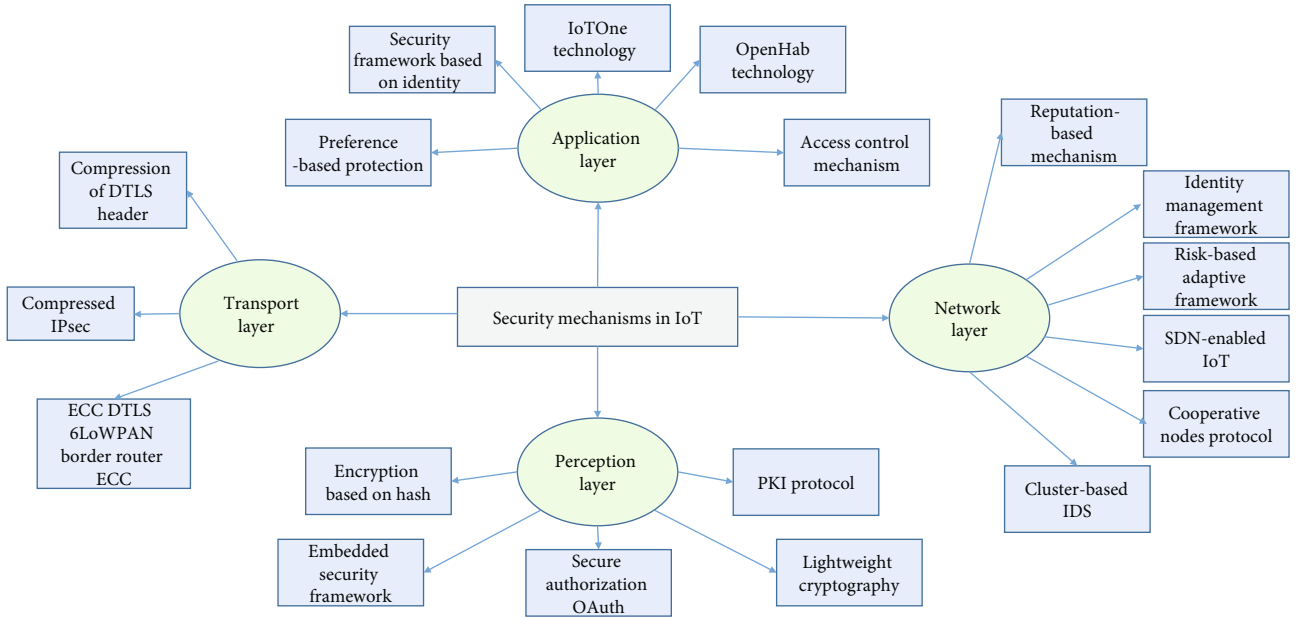

Figure 8: Existing security mechanisms for the protection of IoT applications [42, 51, 105, 107, 109, 111, 112, 114, 115, 117–120, 122, 124, 216].

to the dynamic to pology of the IoT systems which allows the frequent movement of the IoT nodes in and around the network. Different devices working in this layer use sensors and RFIDs. Because of their limited adequacy from the storage and computational point of view, these devices are prone to different kinds of security threats [41, 99]. Various kinds of devices operating in this layer are susceptible to replay attack, timing attacks, node capture attacks [45], and DoS attacks. All these security challenges can be dealt with by encryption, access control, and authentication [100]

(ii) Security threats in the network layer: along with the DoS attacks discussed previously, the network layer of an IoT system can also be targeted for silent monitoring, traffic analysis, and eavesdropping. The major reasons behind these attacks are the remote access and exchange of data. The vulnerability of this layer to a man-in-the-middle attack is terrific [41]. An unsecure communication channel is the root cause of eavesdropping. Communication technologies and protocols play a major role in stopping eavesdropping and further stopping identity theft. As the heterogeneity of devices is a major issue in the IoT systems, it is the biggest challenge to have more secure protocols in the network layer to deal with this diversity. Attackers also misuse the connectivity of the devices to steal user information for future attacks [101]. Along with ensuring the security of the network from the attackers, ensuring the security of the devices operating in the network is equally important. Consequently, the devices in the network must have the comprehension to safeguard themselves against network attacks. This can be obtained only with secure network protocols as well as smart applications [102]

(iii) Security threats in the application layer: lack of standard policies related to IoT systems causes many security challenges in the IoT applications and their development. As a variety of authentication mechanisms are used in different IoT applications, it is difficult to warrant data security and user authentication. The second major challenge is how to deal with the interaction of the user with applications, how to deal with the volume of data exchanged, and how to manage the different applications. The IoT users must be checked to confirm what they wish to share about themselves and how that information is to be used and by whom [42]

(iv) Security threats in the transport layer: common threats in the transport layer include cross-site scripting (XSS). In this type of attack, the malicious user injects client-side-based scripts like Java, HTML, or VBScript into a webpage that is frequently visited by the user. These scripts will be masked as valid requests between the browser (client-side) and the webserver. It can lead to data theft and manipulation. The other attacks include session hijacking, cross-site request forgery (CSRF), and Lightweight Directory Access Protocol (LDAP) injection [103]

Table 4 describes the taxonomy of various attacks and defence mechanisms at different layers of IoT devices.

4.6. IoT Security Mechanisms and Measures. Security is a demanding affair that persists in IoT systems. The benefits

Table 4: Taxonomy of various attacks and defence mechanism at different layers.

Application layer		Network layer		Perception layer		Transport layer	
Attack	Possible defence mechanism	Attack	Possible defence mechanism	Attack	Possible defence mechanism	Attack	Possible defence mechanism
Common injection attack	OpenHab technology IoTOne technology	Node misbehaviour and service attack	Reputation based	Cipher text attack	Encryption based on Hash	Flooding attack	Compressed DTLS header
Attack on privacy	Preference-based protection	Identity theft attack	Identity management framework	DDoS attack	PKI protocol	Replay attack	Compressed IPsec
Identity spoofing attack	Security framework based on Identity	Fault injection attack	Risk-based adaptive framework	Phishing attack	Secure authorization OAuth	Routing attack	ECC DTLS 6LoWPAN Border router ECC
		Side channel attack	SDN-enabled IoT	Side channel attack	Lightweight cryptography		
		No forwarding attack	Cooperative nodes protocol	Crypt-analysis attack	Framework based on embedded security		
		Eavesdropping	Cluster-based IDS				

of the IoT system cannot be obtained without addressing different security issues [51, 104]. Various security mechanisms proposed by various researchers to safeguard different IoT applications are shown in Figure 8. Different security mechanisms used in the perception layer of the IoT systems are Encryption and Hash-based security [105, 106], Public Key Infrastructure- (PKI-) Like Protocol [107, 108], Secure Authorization Mechanism with OAuth (Open Authorization) [109, 110], Lightweight Cryptographic Algorithms [111], and Embedded Security Framework [112, 113]. The network layer of IoT is protected by the Identity Management Framework [114], Risk-Based Adaptive Framework [115], Association of SDN (Software-Defined Networking) with IoT [116], Cooperation of Node-Based Communication Protocol [117], Reputation System-Based Mechanism [118], and Cluster-Based Intrusion Detection and Prevention System [119]. Various security mechanisms implemented in the application layer of IoT are the Preference-Based Privacy Protection Method [120, 121], Access Control Mechanisms [122, 123], OpenHab Technology, IoTOne Technology [124], and Identity-Based Security [125, 126]. All these security mechanisms about the security provided by the different layers of IoT are compared in Table 5.

5. Role of Digital Forensics in Cybercrime Investigation

Although crime has always persisted in society, the aids used by criminals in committing crimes have evolved and grew more advanced with time. With the advent of technology, criminals have come up with new and technologically advanced methods to commit crimes called cybercrimes. In the past, criminal inquiries depended on the investigation of the physical evidence and crime locations along with witnesses. However, nowadays in the internet era, crime scenes may be comprised of smart IoT devices, computers, etc. [53]. Consequently, the process of criminal investigations may consist of the analysis of digital evidence [127].

5.1. Digital Forensics. Digital evidence may consist of a variety of elements. Primarily, the evidence would consist of smartphones, laptops, computers, hard drives, USB, etc. As everyone can have any of the above devices, a large volume of data will be available for analysis. However, a major hindering factor in the analysis is the variety of formats in which data is available on these different devices [53]. As there is a big change in the type of evidence with time, so there is a need for new techniques to handle this change efficiently. Just like traditional forensics, digital forensics is a domain that interprets digital data [62]. Digital forensics experts collect, preserve, and analyze digital evidence [128]. Rogers states, "The science of digital forensics has developed, or more correctly is developing; while this science is arguably in its infancy, care must be taken to ensure that we do not lose sight of the goal of the investigation process namely identifying the parties responsible" [53, 129]. During the design and development of new techniques to analyze digital evidence, it is mandatory to consider other aiding domains to develop and support in the process of the criminal investigation. A digital forensics approach deploys a framework for the techniques to be used in a digital forensics-dependent investigation [130].

5.2. IoT Forensics in Cybercrime Investigation. The IoT forensics can be observed as a subdomain of digital forensics. IoT forensics is a comparatively new and less scrutinized area. Its fundamental aim falls in line with digital forensics, i.e., to

Table 5: Comparison of existing IoT security mechanisms in different layers.

Method name	Layer	Description	Issues focused on the method
Risk-based adaptive framework	Network	Each portion of the four portions performs its tasks and acknowledges the other.	It keeps watching for attacks. It removes the incoming attack at the second portion [115].
Preference-based privacy protection	Application	The service provider, client, and third party initiate communication in a secure environment.	Between the client and the service provider, the third party acts as a bridge and keeps a check on the security provided to the client through the service provider [121].
OpenHab in the application layer	Application	Provision of security.	The device mismatch is not supported but registration is simple [124].
PKI protocol	Perception	A message is sent by the base station to the destination consisting of a public key.	The message is delivered independently without compromising security [108].
IoTOne	Application	OpenHab technology issues are solved.	A device mismatch is allowed. The request is sent by the client to the server for the verification of the user [124].
Security framework based on identity	Application	Registration, policy, client, and user authentication are part of this system.	Admin describes the policies. Users and all other resources are managed by the framework based on policies [125].
Encryption based on Hash	Perception	Encryption algorithms and Hash functions are used in parallel.	The integrity of the message is checked [106].
Mechanism-based on the secure authorization	Perception	RBAC and ABAC mechanisms and systems are based on client-server.	Resources are provided by the server to the client on request, thus making the system more secure [109].
Lightweight cryptographic algorithms	Perception	Messages are converted by using keys.	Plain text from the message is converted to a cipher using Hash functions and symmetric and asymmetric keys [233].
Embedded framework of security	Perception	Memory operating system and run-time environment are secured.	More secure memory management, secondary storage, and run-time environment to the users [112].
The framework of identity management	Network	Communication is done via service and identity.	Information about the user is confirmed by the identity module to protect the users from the attackers [114].
SDN with IoT	Network	Low cost and lesser hardware are used for better performance.	IoT agents and controllers are provided security by SDN as all communications are done through SDN [116].
Mechanism-based on reputation	Network	Data structures, namely, the reputation table and watchdog mechanism, are maintained by the node to prevent intruders.	Ad hoc communication-based system [118].
Heterogeneous fusion mechanism in IoT	Transport	Prevents disclosure of data and information.	Roaming authentication security in the heterogeneous environment [234].

collect and analyze digital evidence legally and accurately [62]. In IoT forensics, data could be collected from sensors, IoT devices, networks, and clouds [131]. IoT forensics can be categorized as device-level forensics, network forensics, and cloud forensics, as shown in Figure 9.

The basic contrast between digital forensics and IoT forensics depends upon the devices examined in crime investigation. In digital forensics, the various devices under examination may be computers/laptops, servers, tablets, and smartphones [132]. Although IoT forensics has a wider area of applicability like smart homes, smart vehicles, drones, and general IoT systems, the published literature on the area of applicability of IoT forensics is less than that of digital forensics.

(i) Smart homes: it has been observed that during criminal investigation, smart home devices can provide compromising information [133]. Usually, the main components of these devices are microphones and motion detectors. These devices play a major role in identifying the location of suspects. There are three main categories of devices to collect forensics: active, passive, and single-malicious active. In [133], two smart devices, i.e., light and bulb, have been experimented by the authors. It has been observed that a large amount of data can be collected even with these passive devices, which can help to identify the activity executed at a specific timestamp. The design of another smart home solution, i.e.,

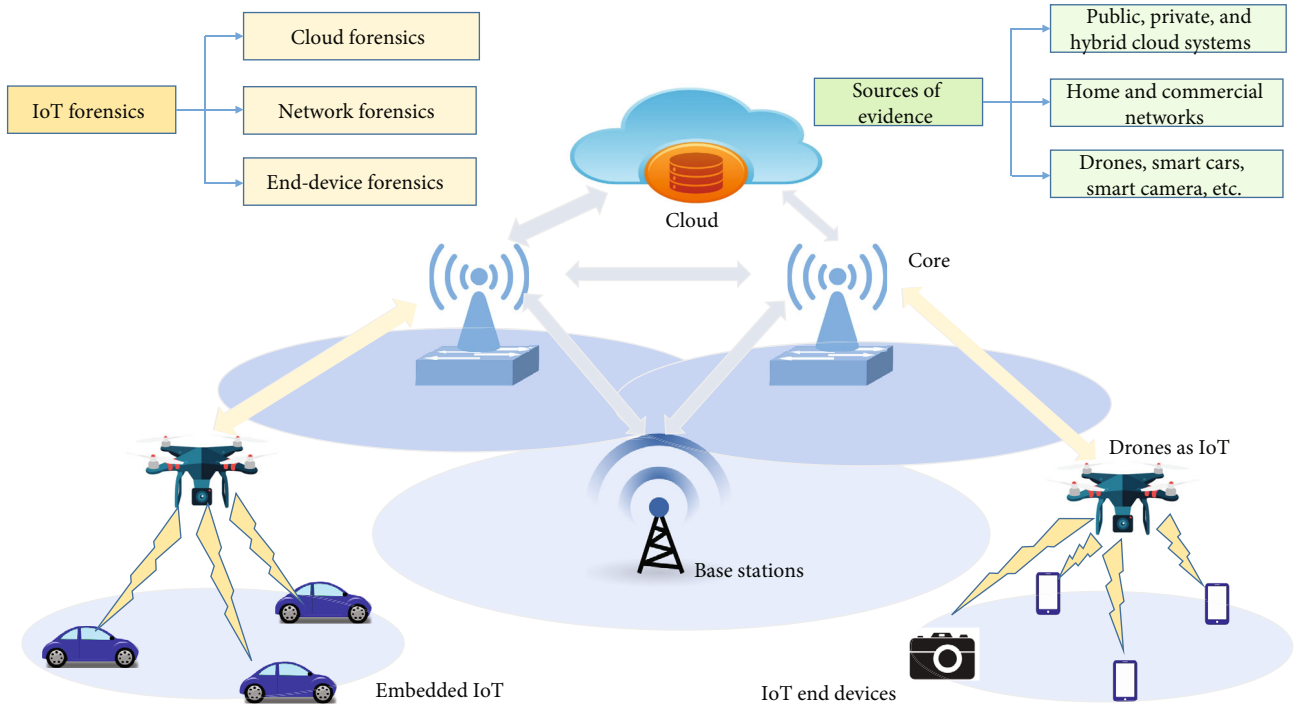

Figure 9: IoT forensic components [62, 128, 131, 217, 218].

the Forensics Edge Management System (FEMS), is discussed in [134]. The focus of the proposed system is to administer security in smart homes along with forensics assistance. Although it has a variety of features ranging from automatic detection to intelligence and flexibility, this system has two main limitations, i.e., complex implementation and testing. The authors in [135] presented security concerns in smart devices. It is impressive that the security threat in an IoT environment increases with an increase in the number of devices in the network. Consequently, the need for IoT forensics arises. In this case study, special attention is given to the IoT forensics in smart homes. The authors also highlighted the need for advanced IoT forensics because of the different IoT challenges. It is expected that in the coming future, smart homes will become widespread. Therefore, a seven-step methodology is proposed for easy investigation in smart home surroundings [136]. It is highlighted by the authors that the proposed framework assists in evidence collection and storage. However, it needs to be tested with a true home automation system

(ii) Smart city and vehicle automation: smart cities are computerized environments, also termed cyberphysical ecosystems, that enhance the utility of traditional city infrastructure like parking spaces, power grids, and gas pipes [62, 137]. In this way, better services can be provided to the residents [138, 139]. One important example, i.e., smart parking, is an area of major concern for most city administrations and auto-tech companies [140]. The network of smart vehicles assists the exchange of information between the vehicles and the environment [132]. These smart vehicles have aided various important areas like road safety and traffic administration. However, they have also raised many issues concerning digital forensics. In a case study [141], a new framework named "Trust—Internet of Vehicles (IoV)" is proposed by the authors for dependable investigation. It assists in gathering and saving dependable evidence from a network of tremendously scattered smart vehicles [142]. This framework is also very useful in preserving evidence and assuring the integrity of the saved evidence. In [143], various threats to smart vehicles are reviewed by the authors. The authors also proposed and tested a new technique to investigate smart vehicles. However, this technique still needs to be validated with the data produced by a network of smart vehicles in an actual scenario

(iii) Drone forensics: in [144], the authors proposed a new approach for the forensic analysis of data gathered through drones. The reference data used for forensic analysis were collected from the DJI Phantom III drone. Drone Open-Source Parser (DROP), a new tool to format the data and prepare for internal storage of the system, is also proposed. The authors elaborated that the drone is controlled with the help of mobile and various types of data files that are also found on the controlled mobile phone. The data collected in these files aid to identify the location, flight time, and other related information of the drone under observation. However, the main

limitation of the work is that it focused only on one type of drone; so, work needs to be extended to other types too

(iv) Cloud forensics: cloud forensics acts as a backbone to IoT forensics. In [145], the authors proposed a new technique to gather and analyze data from the newer BitTorrent Sync peer-to-peer cloud storage service [146]. The data is generated by experimenting with a variety of diverse smart systems. The authors observed that data stored in various log files, installation records, and metadata can be recovered. It is highlighted that the state of the data in memory should be conserved for accurate forensic analysis. However, the proposed method has not been legitimized by actual device manufacturers [147]

(v) Smartphone forensics: in the modern era, people are highly dependent on smartphones. Smartphones play a major role in the exchange of text and audio and video data. Criminals can commit different types of crimes using smartphones like transaction fraud, harassment, child trafficking, and pornography. It is very difficult to elicit data related to the above activities from smartphones for forensic analysis. To solve this issue, the authors conducted a study [148]. In their study, the Samsung Galaxy S3 phone was used as the device for the experiment used for data extraction. It has been observed that to transplant a mobile phone is a tedious activity as it is always associated with risk, i.e., damage to PoP components. The authors in [148] proposed a new methodology named PoP chip-off/TCA. This methodology aids in the transplantation of mobile phones. A new technique was designed and experimented for the successful forensic transplantation of a cryptographic Blackberry 9900 PGP mobile phone

(vi) Healthcare forensics: the healthcare sector is one of the domains most prone to major security threats. The main reason for this is the diverse nature of medical applications and the heterogeneity of the types of equipment used; thus, it has a broader surface for attacks [62, 149]. Besides the evolution in the healthcare industry that plays a major role in the development of human life, various smart health monitoring systems also put the security of a patient's medical data at risk. IoT-based fitness systems could be targeted by attackers to steal the data of the users, which can be further misused [150]. Numerous medical identity thefts have been identified in the past which express the importance of medical data. In the domain of medical health services and applications, a compound annual growth of 29-30% is expected from the year 2019 to 2025 [151]. Many fitness wearables can be used as a source of evidence in criminal investigations as these gadgets keep on storing the data related to routine activities of the users at the back end passively. Thus, although these gadgets were designed to maintain the health status of the users, it can also be used as digital evidence [14]. The number of users, smart watches, and fitness bands are increasing day by day; so, the study of these IoT devices has become the center of interest for forensics practice. According to the authors in [152], the data extracted from these gadgets may be personal to the users. Therefore, special attention should be given to the security of this data. As the number of security-related issues is increasing exponentially, there is a requirement of more advanced techniques to ensure the security of data [153]

(vii) General IoT system forensics: in [14], the authors came up with a new investigation platform for diverse IoT systems. A risk judgment scheme dependent on STRIDE and DREAD methods was designed and modeled. It was discussed with the help of these two exemplary models that cybercrime committed in the IoT environment can even cause serious risks like death. It was observed by the authors that most of the IoT systems are not deployed with default security measures; so, it possesses high risk. A study was carried out [154] to analyze the significance of the sync data in evidence analysis. Sync data contributes to the fair investigation of the digital witness. A survey was conducted [155] by the authors to study and analyze forensics investigation techniques for data stored in the system memory. Few meaningful alterations to the operating systems were also impressed upon in this study. In [156], data contraction and partially automated analysis techniques to handle a large volume of digital evidence were suggested. This technique assists in the analysis of a variety of IoT data gathered. In [157], the authors discussed the approaches of gathering, saving, and communicating digital evidence in a secure way to a genuine destination. Some technologies to bring it into practice were also highlighted by the authors, along with the basic components of the electronic evidence that were also described

In [158], a novel approach to club cloud-native and cloud-centric forensics for the Amazon Alexa ecosystem was proposed. A new framework named "Probe-IoT" is presented in [159], which aids in identifying criminal evidence in the IoT environment using electronic logs. These logs preserve the complete information regarding all data exchanges between things, users, and cloud services. This framework was not tested experimentally, but it conceptually safeguards the integrity of the evidence. In [160], the authors presented a novel model for IoT forensics named PRoFIT to ensure the implementation of standards during forensic analysis. This model was tested in a true IoT environment deployed in a coffee shop. The 1-2-3 zone approach is applied by the authors [161] for IoT forensic analysis. According to the

authors, concerned persons and pieces of evidence fall into zone 1, things or devices near to the boundary of the network fall into zone 2, and devices exterior to the network are capped in zone 3. This approach was developed to support accurate IoT investigation. However, the practical implementation of this approach is comparatively challenging. The authors in [162] presented a new framework dependent on a three-layer architecture. The proposed framework has many advantages to ensure data security with only one disadvantage, that is, it is not much suitable in coping with the limited resources of IoT devices like processing power and battery life. The researchers in [163] proposed a design of a new model to help forensic experts in IoT evidence analysis. This model was proposed to preserve volatile data in IoT devices. This work was planned as an extension of previous research. Using this model, forensic experts can investigate a broader surface in the data domain. However, it has been observed that this model is laborious to implement in a true environment. In [164], the authors presented IoT forensics in a new way. In this work, the IoT domain was methodically explored to disclose the various challenges in the domain of digital forensics. A novel technique named Forensic Aware IoT (FAIoT) was introduced with a focus on uncovering new details in an IoT environment. However, the applicability of the approach is doubtful as it was not verified in the IoT environment. The authors [165] analyzed prominent technical issues in digital forensics which can hinder the identification of important facts for investigation. Various research issues, which can significantly improve the process of digital forensics, were also highlighted. Different types of attacks that are frequently planned on the devices in an IoT environment were discussed in [166] along with the complexity which they add to the digital investigation. The hackers use a large number of random UDP attacks at the same time by using UDP datagrams of varying sizes. Consequently, the attacks caused denial of service. The authors introduced a novel approach to handle these types of attacks by identifying their originators. A number of patents have been granted in the development of digital forensics in the past. Table 6 presents the patents granted in recent years. Many applications of digital forensics have been developed to prevent cybercrime. Table 7 presents the list of real-time digital forensics applications that support various operating systems and other platforms to prevent cybercrime in IoT devices.

6. Advanced IoT Security

Smart devices and applications in various areas of IoT make human life more comfortable, but they also make IoT systems more vulnerable to cyberattacks. These devices and applications are connected to the internet, which creates new opportunities for cybercriminals to enter the IoT environment. Cybercriminals can enter an IoT system through routers and can damage it in many ways. Although several security mechanisms are available in IoT, advanced technologies like artificial intelligence (AI), machine learning (ML), neural networks (NN), blockchain technology, fog computing, and edge computing are playing a major role to handle cyberattacks and helping to control cybercrime [167, 168]. Authors in [169] discussed in brief the various kinds of security threats in an IoT environment. The need for a dynamic and quick system to safeguard the IoT systems against cybercrime is impressed upon. The authors proposed a hybrid system to detect cyberattacks using AI and ML in a cloud computing environment. Both types of attacks, i.e., at the device level and the network level, can be detected with this model. According to the authors, it is considered by the security experts that AI and ML provide very powerful security mechanisms as even future attacks may be predicted based on past IoT attack data. Consequently, this system does not wait for the occurrence of attacks but it can predict them in advance. The main limitation of the system is that it can work only with standard data formats for prediction. ML provides solutions to DoS attacks, eavesdropping, spoofing, and privacy leakage in an IoT environment [170]. The authors in [171] presented a multilayer architecture to associate the various devices within IoT to make them accessible throughout the network at all times. To deal with the security issues of end nodes and to provide more credible services, a novel framework using NN was proposed. According to this framework, security issues need to be tackled in each layer of the IoT architecture. Each end node configured using this framework will have the potential to self-monitor and recover after any unwanted event/attack. In the proposed framework, a NN-based adaptive model was used for the automatic recovery of the nodes. In [172], the authors presented an artificial neural network (ANN) approach to control distributed denial of service (DDoS) attacks. The ANN was tested in a simulated IoT environment. The results obtained with the proposed technique were found to be 99.4% accurate, and this technique is capable of identifying numerous DDoS/DoS attacks. The authors in [170] highlighted that the incorporation of blockchain in IoT systems has numerous benefits. The distributed architecture of blockchain reduces the risk of failure of data storage nodes. Thus, it leads to more secure data storage in the IoT environment [173, 174]. The concept of data encryption is used by blockchain for data storage in the IoT environment; so, there are less chances of storing damaged data in things [175]. The augmentation of blockchain with IoT also helps to prevent unauthorized access, data loss, and spoofing attacks [176]. Various challenges in IoT along with the workable solutions administered by the blockchain technology are discussed below in Table 8.

In [170], the authors discussed that a large volume of data is generated by diverse devices in the IoT environment. It is very taxing to shift the entire data to the cloud for real-time analysis; thus, the concept of fog computing evolved. Under this concept, the cloud framework is extended to the edge of the network [177]. Fog computing can handle various IoT security attacks like the man-in-the-middle attack, data transit attacks, eavesdropping, and resource constraint issues very efficiently [178]. The various characteristics and possible solutions deployed by fog computing are shown in Figure 10. Authors in [170] noted that the edge computing framework is an expansion of cloud computing. The location of the computational power and analysis mechanisms differentiate edge computing from fog computing in an IoT environment

Table 6: Various patents granted in the development of digital forensics.

Patent title	Year Filed	Year Published	Inventor	Country	Key features
Differencing engine for digital forensics	2018	2020	Monsen and Glisson [235]	US	Anomaly detection to mitigate the security attack on cloud-based servers.
Forensic investigation tool	2017	2019	Jon D. McEachron [236]	US	Digital investigation tool capable of recovering and decrypting the content.
Forensic system, forensic methods, and forensic program	2015	2016	Morimoto et al. [237]	US	A medium to acquire and analyze the digital information in a server or a plurality of computers.
Devices and methods for providing security in a remote digital forensic environment	2016	2017	Kang et al. [238]	US	A method for collecting digital evidence from the target system. Analysis of the collected evidence to be done at a remote location.
Method and apparatus for digital forensics	2008	2012	Choi et al. [239]	US	A method to perform digital forensics by extracting page files from the target stored medium. Also, extract features from the extracted page file.
Systems and methods for provisioning digital forensics services remotely over public and private networks	2012	2015	Shannon and Decker [240]	US	A method to collect and analyze electronically stored information over public and private networks using cloud computing.
Digital forensics	2009	2014	Buchanan et al. [241]	US	System call information is acquired from the device under test. The acquired data is converted into a sequence format for further investigation.
Methods for data analysis and digital forensics and systems using the same	2011	2014	Gil et al. [242]	US	It comprises an online data forensic server to acquire and analyze the usage history of a device. It also issues a timestamp to the collected data.
Forensic digital watermarking with variable orientation and protocols	2001	2008	K. Levy [243]	US	A method of forensic digital watermarking on the randomly selected orientation in the content signal.
Secure digital forensics	2007	2011	Carpenter and Westerinen [244]	US	To perform an audit of computer processor status and memory, a security module is designed. This can be done using a separate hardware path to access the processor register data through a debug port.

[179]. In edge computing, both these potentials reside at the edge [180]. The various devices in the IoT system coordinate to establish a network and perform various computations required for data analysis within that network [181]. Therefore, the need to communicate the data outside the device is reduced which contributes to improved data security in the IoT applications. On the same grounds, this framework also aids in minimizing the communication cost of data [182]. The concept of edge computing helps to handle data breaches, data compliance issues, safety issues, and bandwidth challenges in an IoT environment [183].

7. Road Map of Problems in IoT Forensics

IoT forensics is a complicated and regularly emerging domain. It plays a very crucial role in cybercrime investigation. However, many challenges need to be addressed very carefully. These challenges open the doors for further research in the field of IoT forensics [62]. Thus, the main objective of this section is to show a path to the researchers in the domain of IoT forensics to aid in cybercrime investigation. These include the following:

(i) Data locations: in IoT systems, the data are saved at various locations in dynamic devices that may be regulated by different administrations. Consequently, the investigators undergo serious problems trying to identify which regulations are to be followed when the device was used to commit a crime [184]. In this type of situation, crime investigation becomes a more complicated task. So, there is a need for standard processes and mechanisms to address this issue

(ii) Forensic automation: there are numerous technical issues faced during automated IoT forensic analysis. The major problems which affect the process are the dynamic nature of the devices and the involvement of advanced methods in the process

Table 7: List of real-time digital forensics applications to prevent cybercrime.

Software	OS/Support	Features	Sources
E3 Universal	Window, Linux, macOS, iOS	IoT analysis, cloud data imaging, and analysis, registry analysis, email investigation, JTAG, and chip dump processing	https://paraben.com/digital-forensic-tools-6/
WireShark	Windows, Linux, macOS, Solaris	VoIP, GUI, offline analysis, WAN/LAN analyzer	https://www.wireshark.org/
Autopsy	Windows, Linux, macOS Android	Registry analysis, LNK file analysis, timeline analysis, file type detection, email analysis	https://www.sleuthkit.org/autopsy/
Paladin	Linux	Device cloning support for many forensic image formats: E01, Ex01, RAW, VHD, AFF, disk manager, and automatic logging	https://sumuri.com/software/paladin/
Dumpzilla	Unix, Windows	Forensic information extraction from Firefox, SeaMonkey browsers including cookies, bookmarks, web forms, SSL certificates, browser-saved passwords	https://tools.kali.org/forensics/dumpzilla
SIFT (SANS investigative forensic toolkit)	Linux	File system support, different evidence image format support, rapid scripting, and analysis	https://digital-forensics.sans.org/community/downloads
Toolsley	Web based	File repairing, text encoding, file identification, file signature verification, binary inspection, CRC tool	https://www.toolsley.com/
NetworkMiner	Windows, Linux, macOS X, FreeBSD	Live sniffing, OS fingerprinting, Geo IP localization, DNS whitelisting, audio extraction and playback of VoIP calls, PCAP and PcapNG file parsing	https://sectools.org/tool/networkminer/
Elcomsoft	Windows, macOS, iOS	Password recovery, cloud explorer, disk decryption, wireless security auditor	https://www.elcomsoft.co.uk/
Belkasoft X	Windows macOS, Linux, iOS, Android, Blackberry	E01/DD imaging, Hash set analysis, registry viewer, plist viewer, artifacts viewer, SQLite viewer	https://belkasoft.com/

Table 8: Theoretical solutions offered by deploying blockchain in the IoT framework to prevent cyberattacks.

Challenges in IoT	Specifications	Theoretical blockchain solution
Defects in architecture	A point of failure exists in IoT devices that affect the device and the network.	Validation can be done using blockchain. The data is also verified through cryptography to ensure that a legitimate sender has sent it [245].
Manipulation of data	The data extracted from IoT devices is manipulated and is used inappropriately.	Using blockchain, the IoT devices are interlocked due to which the system rejects any kind of change in data through IoT devices [246, 247].
Service inefficiency due to heavy load on the cloud server	Cloud services malfunctions due to cyberattack, power failures, or bugs in software.	Data records are uploaded on different nodes on the network. Due to the same data in different nodes, there is no single point of failure [248, 249].
Traffic and cost management	The handling of the exponential growth in IoT devices is a tedious task.	The IoT devices can be connected and communicated through peers bypassing the central servers through the decentralization feature [250, 251].
Privacy issues in IoT devices	The user data present in IoT devices are more vulnerable due to cyberattacks.	The permissioned blockchain can eradicate this problem [252–254].

of forensic investigation. To obtain a real-time solution to the problem, there is a requirement for improved IoT automation. The authors in [134] presented a novel direction for IoT forensics by introducing an automated technique for forensics examination. It is also impressed upon by the authors that the diversity of IoT devices is the main hindrance in the real-time implementation of the proposed technique. Therefore, some standard mechanisms are required to deal with the heterogeneity of the devices and collected data

(iii) IoT device management: in an IoT environment, sometimes a particular device malfunctions and starts generating malignant data. Although shutting that device down may be required, it may not be feasible for the forensic investigator to do so because of the owner's decision. In a smart home, for example, even if a washing machine is initiating vengeful data packets, the owner may not pass his consent to stop it as it may disturb his daily routine. This may lead to a big challenge for the expert crime investigator. Therefore, due attention needs

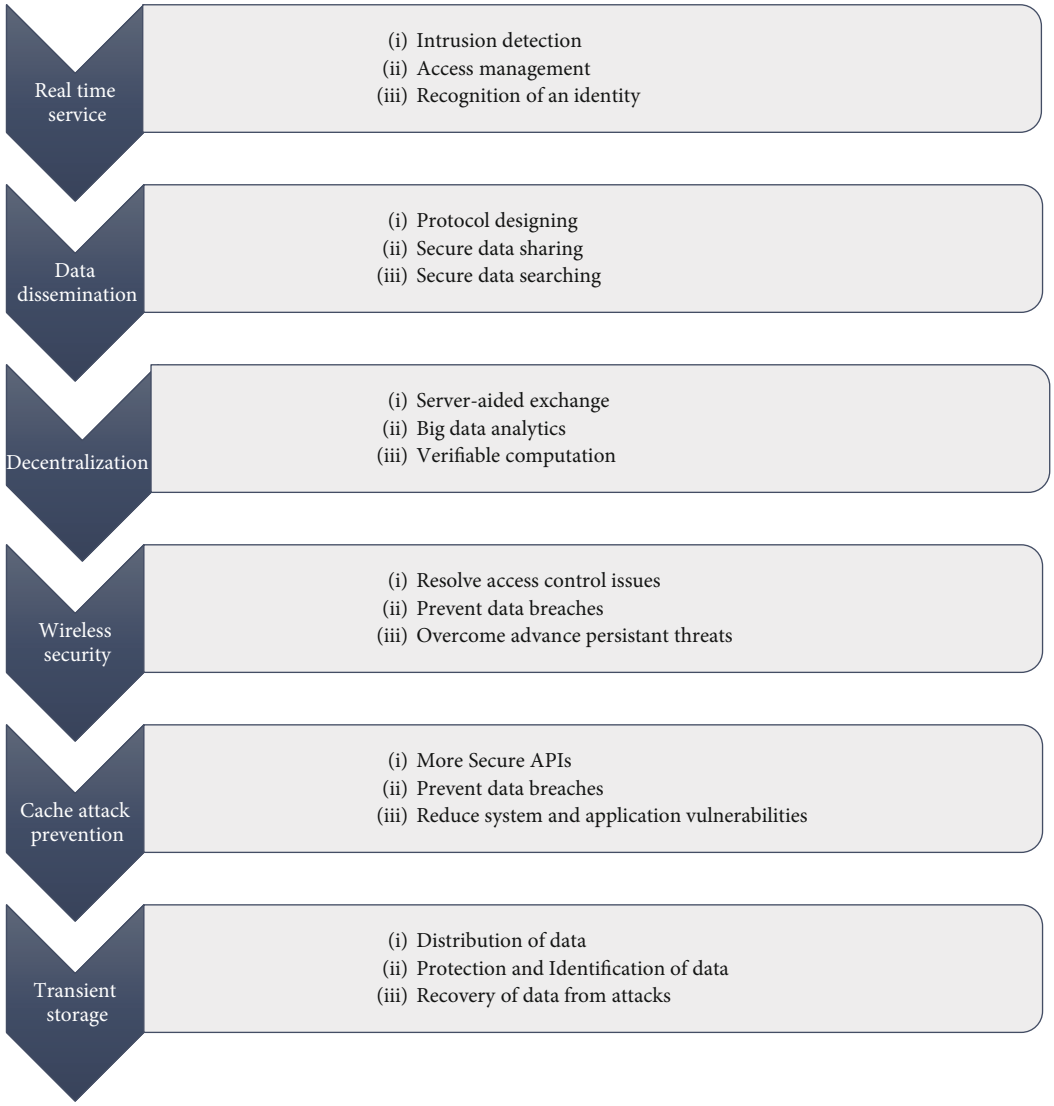

Figure 10: Possible solutions offered through fog computing [219–230].

to be given to design the required mechanisms to provide the crime investigators freedom of forensic investigation without the cessation of the continued operation of things

(iv) Forensic analysis of data in IoT: forensic investigators deal with a large volume of IoT data using various analysis techniques during the process of crime investigation [185]. In an IoT environment, the data are collected and analyzed from various devices and the results are used for various types of decision making [186]. As the process of data analysis and interpretation is complex, the accuracy of the results and further investigation is affected [156]. Therefore, the need for more standardized, simple, and accurate data analysis tools and techniques arises

(v) Scope and life of digital forensic evidence: the limited storage of IoT devices deters the availability of evidence for a long time which results in the loss of crucial data related to cybercrimes [131]. To overcome this problem, forensic data should be transferred frequently to the cloud. However, the process of data transfer gives rise to another challenge of ensuring that evidence has not been manipulated during the process. Another major issue is related to the visibility of the evidence. The presence of a few malignant sensors at the crime scene may affect the work of forensic investigators to locate the witness equipment. Log files from various devices may assist the forensic experts; however, these may not necessarily provide the complete set of evidence for the investigation

(vi) Privacy of the user: the entanglement of IoT devices in various domains has made human life very comfortable. However, it has put the privacy of the users of smart devices at stake. It has been observed that there is a lack of privacy-specific forensic

mechanisms for the IoT environment [187]. The main loophole of most of the available forensic solutions is that the privacy aspect of the users is ignored during the process of investigation [188]. All investigation solutions proposed in [157, 160, 189] have serious privacy challenges. In very diverse and dynamic IoT systems, the practice of suitable privacy measures can enhance the involvement of digital evidence for cybercrime investigations

(vii) Security in IoT devices: the diverse nature of devices in the IoT environment opens a new space for unauthorized users to attack the system which is very difficult to identify during the forensic investigation. Consequently, the process of collecting evidence becomes more tedious. Therefore, it is essential that during the design of various forensic investigation mechanisms, the diverse nature of IoT systems should be kept in mind [190]. The authors introduced the concept of security and privacy in [56, 191]. The proposed approaches and algorithms provide more liberty to forensic investigators by leaving aside security issues. By considering the diverse and dynamic nature of the IoT environment, more of such techniques are needed in cybercrime investigation [192, 193]

(viii) Other issues and future research: during the study of various challenges, it has been observed that there is a requirement for more standardized techniques and mechanisms in administering the data gathered from heterogeneous and dynamic devices to facilitate the process of cybercrime investigation. Due to the diversity of the formats of the data gathered from the various devices, there is also a requirement for more sophisticated data analysis tools and techniques. Advanced methods need to be proposed to facilitate the liberty of investigators to work without interrupting the operations of smart devices and equipment. As the storage capacity of most of the smart devices is limited, there is a requirement for accurate and efficient techniques to transfer the forensic data from IoT devices to the cloud without any loss of evidence. Suitable measures also need to be practiced ensuring the privacy of the user's personal data during the process of investigation

8. Conclusions

IoT is a developing technology, which has bestowed human life with comfort. However, the growing practice of IoT devices in various domains related to business and personal life has put personal and data security at greater risk. A large volume of data is exchanged openly among the various smart devices in an IoT environment which attracts hackers to penetrate the security system. The dependence of IoT systems on wireless communication technologies makes them prone to cyberattacks which is the root cause of cybercrime. In this paper, we present the various elements of the IoT framework like architecture, protocols, technologies, and application domains. A detailed review of the security aspects of an IoT environment from the years 2010 to 2020 is presented. Various security aspects which may facilitate intruders to commit cybercrime are also discussed. Implementation of the security mechanisms at each layer of the IoT architecture is presented in this survey. The role of IoT forensics and advanced technologies in cybercrime investigation is impressed upon in this review. This survey also consists of patents reported and real-time applications developed to mitigate the problems occurring due to cybercrime in IoT devices. Lastly, the various open research challenges to be addressed are discussed to facilitate the process of cybercrime investigation in the IoT systems.

Data Availability

Any data or material used in the survey is referred to in the article.

Conflicts of Interest

There is no conflict of interests to declare.

References

[1] I. Butun, P. Osterberg, and H. Song, "Security of the internet of things: vulnerabilities, attacks, and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 616–644, 2020.

[2] V. Sharma, G. Choudhary, Y. Ko, and I. You, "Behavior and vulnerability assessment of drones-enabled industrial internet of things (IIot)," *IEEE Access*, vol. 6, pp. 43368–43383, 2018.

[3] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[4] S. Forsström, I. Butun, M. Eldefrawy, U. Jennehag, and M. Gidlund, "Challenges of securing the industrial internet of things value chain," in *2018 Workshop on Metrology for Industry 4.0 and IoT*, pp. 218–223, Brescia, Italy, April 2018.

[5] S. Jeschke, C. Brecher, H. Song, and D. Rawat, *Industrial Internet of Things: Foundations, Principles and Applications*, Springer, Cham, Switzerland, 2017.

[6] H. Song, D. B. Rawat, S. Jeschke, and C. Brecher, *Cyber-physical Systems: Foundations, Principles and Applications*, Morgan Kaufmann, 2016.

[7] P. V. Astillo, J. Kim, V. Sharma, and I. You, "SGF-MD: behavior rule specification-based distributed misbehavior detection of embedded IoT devices in a closed-loop smart greenhouse farming system," *IEEE Access*, vol. 8, pp. 196235–196252, 2020.

[8] A. Kataria, S. Ghosh, V. Karar, T. Gupta, K. Srinivasan, and Y.-C. Hu, "Improved diver communication system by combining optical and electromagnetic trackers," *Sensors*, vol. 20, no. 18, p. 5084, 2020.

[9] V. Sharma, R. Kumar, and R. Kaur, "UAV-assisted content-based sensor search in IoTs," *Electronics Letters*, vol. 53, no. 11, pp. 724–726, 2017.

[10] I. You, H.-C. Chen, V. Sharma, and I. Kotenko, *Mobile Internet Security: Second International Symposium, MobiSec 2017*, vol. 971, Springer, Jeju Island, Republic of Korea, 2018, October 19–22, 2017, Revised Selected Papers.

[11] Y. Lu and L. D. Xu, "Internet of things (IoT) cybersecurity research: a review of current research topics," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2103–2115, 2019.

[12] F. Servida and E. Casey, "IoT forensic challenges and opportunities for digital traces," *Digital Investigation*, vol. 28, pp. S22–S29, 2019.

[13] V. R. Kebande, N. M. Karie, A. Michael, S. M. G. Malapane, and H. S. Venter, "How an IoT-enabled "smart refrigerator" can play a clandestine role in perpetuating cyber-crime," in *2017 IST-Africa Week Conference (IST-Africa)*, pp. 1–10, Windhoek, Namibia, May 2017.

[14] N. Akatyev and J. I. James, "Evidence identification in IoT networks based on threat assessment," *Future Generation Computer Systems*, vol. 93, pp. 814–821, 2019.

[15] A. K. Singholi, M. Mittal, and A. Bhargava, "A review on IoT-based hybrid navigation system for mid-sized autonomous vehicles," in *Advances in Electromechanical Technologies*pp. 735–744, Springer.

[16] A. Abdullah, R. Hamad, M. Abdulrahman, H. Moala, and S. Elkhediri, "CyberSecurity: a review of internet of things (IoT) security issues, challenges and techniques," in *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, pp. 1–6, Riyadh, Saudi Arabia, May 2019.

[17] A. Venčkauskas, R. Damaševičius, V. Jusas, J. Toldinas, D. Rudzika, and G. Drėgvaitė, "A review of cyber-crime in internet of things: technologies, investigation methods and digital forensics," *International Journal of Engineering Sciences and Research Technology*, vol. 4, pp. 460–477, 2015.

[18] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in internet-of-things (IoTs) framework," *Future generation computer systems*, vol. 108, pp. 909–920, 2020.

[19] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé, "Vision and challenges for realising the internet of things," *Cluster of European Research Projects on the Internet of Things, European Commision*, vol. 3, pp. 34–36, 2010.

[20] G. Marias, J. Barros, M. Fiedler et al., "Security and privacy issues for the network of the future," *Security and Communications Networks*, vol. 5, no. 9, pp. 987–1005, 2011.

[21] K. Liebrand, K. Moser, S. Knüsli et al., "Ethics, privacy and data protection in BUTLER," *Project Title: Ubiquitous, Secure Internet-of-Things with Location and Contex-Awareness, Project No: 287901*, SWC, 2013.

[22] D. Patel, K. Srinivasan, C.-Y. Chang, T. Gupta, and A. Kataria, "Network anomaly detection inside consumer networks—a hybrid approach," *Electronics*, vol. 9, no. 6, p. 923, 2020.

[23] V. Sharma, I. You, R. Kumar, and V. Chauhan, "OFFRP: optimised fruit fly based routing protocol with congestion control for UAVs guided ad hoc networks," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 27, no. 4, pp. 233–255, 2018.

[24] V. Sharma, D. N. K. Jayakody, I. You, R. Kumar, and J. Li, "Secure and efficient context-aware localization of drones in urban scenarios," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 120–128, 2018.

[25] A. Nieto and J. Lopez, "Analysis and taxonomy of security/-QoS tradeoff solutions for the future internet," *Security and Communication Networks*, vol. 7, no. 12, p. 2803, 2014.

[26] J. Sutanto, E. Palme, C. H. Tan, C. W. Phang, and Fudan University, "Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users," *MIS quarterly*, vol. 37, no. 4, pp. 1141–1164, 2013.

[27] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security challenges in the IP-based internet of things," *Wireless Personal Communications*, vol. 61, no. 3, pp. 527–542, 2011.

[28] N. E. Marion, "The council of Europe's cyber crime treaty: an exercise in symbolic legislation," *International Journal of Cyber Criminology*, vol. 4, p. 699, 2010.

[29] H. Saini, Y. S. Rao, and T. C. Panda, "Cyber-crimes and their impacts: a review," *International Journal of Engineering Research and Applications*, vol. 2, pp. 202–209, 2012.

[30] Y. Zhang, Y. Xiao, K. Ghaboosi, J. Zhang, and H. Deng, "A survey of cyber crimes," *Security and Communication Networks*, vol. 5, no. 4, p. 437, 2012.

[31] M. Felson and R. V. Clarke, "Opportunity makes the thief," *Police Research Series, Paper*, vol. 98, pp. 1–36, 1998.

[32] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[33] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: vision, applications and research challenges," *Ad hoc networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[34] I. You, S. Kwon, G. Choudhary, V. Sharma, and J. Seo, "An enhanced LoRaWAN security protocol for privacy preservation in IoT with a case study on a smart factory-enabled parking system," *Sensors*, vol. 18, no. 6, p. 1888, 2018.

[35] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): a vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[36] C. C. Aggarwal, N. Ashish, and A. Sheth, "The internet of things: a survey from the data-centric perspective," in *Managing and Mining Sensor Data*, pp. 383–428, Springer, 2013.

[37] O. Said, "Accurate performance evaluation of internet multicast architectures: hierarchical and fully distributed vs. service-centric," *KSII Transactions on Internet and Information Systems*, vol. 7, no. 9, pp. 2194–2212, 2013.

[38] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: a survey," *IEEE communications surveys & tutorials*, vol. 16, no. 1, pp. 414–454, 2014.

[39] J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the internet of things: a survey of existing protocols and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015.

[40] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: the road ahead," *Computer networks*, vol. 76, pp. 146–164, 2015.

[41] M. Abomhara and G. M. Køien, "Security and privacy in the internet of things: current status and open issues," in *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)*, pp. 1–8, Aalborg, Denmark, 2014.

[42] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: current status, challenges and prospective measures," in *2015 10th International Conference*

for Internet Technology and Secured Transactions (ICITST), pp. 336–341, London UK, 2015.

[43] J. Pescatore and G. Shpantzer, *Securing the Internet of Things Survey*, SANS Institute, 2014.

[44] D. Gil, A. Ferrández, H. Mora-Mora, and J. Peral, "Internet of things: a review of surveys based on context aware intelligent services," *Sensors*, vol. 16, no. 7, p. 1069, 2016.

[45] F. Muhammad, W. Anjum, and K. S. Mazhar, "A critical analysis on the security concerns of internet of things (IoT)," *International Journal of Computer Applications*, vol. 111, pp. 1–6, 2015.

[46] R. Vignesh and A. Samydurai, "Security on internet of things (IoT) with challenges and countermeasures," *International Journal of Engineering Development and Research, IJEDR*, vol. 5, no. 1, pp. 417–423, 2017.

[47] M. A. Razzaq, S. H. Gill, M. A. Qureshi, and S. Ullah, "Security issues in the internet of things (IoT): a comprehensive study," *International Journal of Advanced Computer Science and Applications*, vol. 8, p. 383, 2017.

[48] C. Maple, "Security and privacy in the internet of things," *Journal of Cyber Policy*, vol. 2, pp. 155–184, 2017.

[49] P. H. Rughani, "IoT evidence acquisition—issues and challenges," *Advances in Computational Sciences and Technology*, vol. 10, pp. 1285–1293, 2017.

[50] G. Corser, G. Fink, and J. Bielby, *Internet of Things (IoT) Security Best Practices; IEEE Internet Technology Policy Community; White Paper*, IEEE, Piscataway, NJ, USA, 2017.

[51] M. Burhan, R. A. Rehman, B. Khan, and B.-S. Kim, "IoT elements, layered architectures and security issues: a comprehensive survey," *Sensors*, vol. 18, p. 2796, 2018.

[52] M. M. Noor and W. H. Hassan, "Current research on internet of things (IoT) security: a survey," *Computer Networks*, vol. 148, pp. 283–294, 2019.

[53] A. MacDermott, T. Baker, and Q. Shi, "IoT forensics: challenges for the IoA era," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1–5, Paris, France, 2018.

[54] A. Riahi Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the internet of things," *Digital Communications and Networks*, vol. 4, no. 2, pp. 118–137, 2018.

[55] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[56] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The effect of IoT new features on security and privacy: new threats, existing solutions, and challenges yet to be solved," *IEEE Internet of Things Journal*, vol. 6, pp. 1606–1616, 2018.

[57] M. Aydos, Y. Vural, and A. Tekerek, "Assessing risks and threats with layered approach to internet of things security," *Measurement and Control*, vol. 52, pp. 338–353, 2019.

[58] S. Nasiri, F. Sadoughi, M. H. Tadayon, and A. Dehnad, "Security requirements of internet of things-based healthcare system: a survey study," *Acta Informatica Medica*, vol. 27, p. 253, 2019.

[59] K. Tabassum, A. Ibrahim, and S. A. El Rahman, "Security issues and challenges in IoT," in *2019 International Conference on Computer and Information Sciences (ICCIS)*, pp. 1–5, Sakaka, Saudi Arabia, 2019.

[60] J. M. Blythe, N. Sombatruang, and S. D. Johnson, "What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?," *Journal of Cybersecurity*, vol. 5, 2019.

[61] F. Adesola, S. Misra, N. Omoregbe et al., "An IOT-based architecture for crime management in Nigeria," in *Data, Engineering and Applications*, pp. 245–254, Springer, Singapore, 2019.

[62] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the internet of things (IoT) forensics: challenges, approaches and open issues," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020.

[63] L. A. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and security: challenges and solutions," *Applied Sciences*, vol. 10, article 4102, 2020.

[64] H. F. Atlam, A. Alenezi, M. O. Alassafi, A. A. Alshdadi, and G. B. Wills, "Security, cybercrime and digital forensics for IoT," in *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, S. L. Peng, S. Pal, and L. Huang, Eds., vol. 174 of Intelligent Systems Reference Library, pp. 551–577, Springer, Cham, 2020.

[65] W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq, and M. K. Khan, "Comprehensive review of cybercrime detection techniques," *IEEE Access*, vol. 8, pp. 137293–137311, 2020.

[66] W. U. Khan, J. Liu, F. Jameel, V. Sharma, R. Jantti, and Z. Han, "Spectral efficiency optimization for next generation NOMA-enabled IoT networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15284–15297, 2020.

[67] V. Puri, A. Kataria, and V. Sharma, "Artificial intelligence-powered decentralized framework for internet of things in healthcare 4.0," *Transactions on Emerging Telecommunications Technologies*, no. article e4245, 2021.

[68] M. U. Sheikh, M. Riaz, F. Jameel et al., "Quality-aware trajectory planning of cellular connected UAVs," in *Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond*, pp. 79–85, London United Kingdom, 2020.

[69] K. Andersson, I. You, R. Rahmani, and V. Sharma, "Secure computation on 4G/5G enabled internet-of-things," *Wireless Communications and Mobile Computing*, vol. 2019, Article ID 3978193, 2019.

[70] D. Shin, V. Sharma, J. Kim, S. Kwon, and I. You, "Secure and efficient protocol for route optimization in PMIPv6-based smart home IoT networks," *IEEE Access*, vol. 5, pp. 11100–11117, 2017.

[71] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of internet of things," in *2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)*, pp. V5-484–V5-487, Chengdu, China, 2010.

[72] C.-W. Tsai, C.-F. Lai, and A. V. Vasilakos, "Future internet of things: open issues and challenges," *Wireless Networks*, vol. 20, pp. 2201–2217, 2014.

[73] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: perspectives and challenges," *Wireless Networks*, vol. 20, pp. 2481–2501, 2014.

[74] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 packets over IEEE 802.15.4 networks," *Internet proposed standard RFC*, vol. 4944, p. 130, 2007.

[75] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: lightweight secure CoAP for the internet of things," *IEEE Sensors Journal*, vol. 13, pp. 3711–3720, 2013.

[76] S. Iren, P. D. Amer, and P. T. Conrad, "The transport layer: tutorial and survey," *ACM Computing Surveys*, vol. 31, pp. 360–404, 1999.

[77] M. A. Sayeed, R. Kumar, V. Sharma, and M. A. Sayeed, "Efficient deployment with throughput maximization for UAVs communication networks," *Sensors*, vol. 20, article 6680, 2020.

[78] J. Zheng and M. J. Lee, "A comprehensive performance study of IEEE 802.15.4," *Sensor Network Operations*, vol. 4, pp. 218–237, 2006.

[79] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: a survey on enabling technologies, protocols, and applications," *IEEE communications surveys & tutorials*, vol. 17, pp. 2347–2376, 2015.

[80] M. Kovatsch, "CoAP for the web of things: from tiny resource-constrained devices to the web browser," in *Proceedings of the 2013 ACM conference on Pervasive and Ubiquitous Computing Adjunct Publication*, pp. 1495–1504, Zurich, Switzerland, 2013.

[81] N. Glombitza, D. Pfisterer, and S. Fischer, "LTP: an efficient web service transport protocol for resource constrained devices," in *2010 7th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, pp. 1–9, Boston, MA, USA, 2010.

[82] M. A. da Cruz, J. J. Rodrigues, E. S. Paradello, P. Lorenz, P. Solic, and V. H. C. Albuquerque, "A proposal for bridging the message queuing telemetry transport protocol to HTTP on IoT solutions," in *2018 3rd International Conference on Smart and Sustainable Technologies (SpliTech)*, pp. 1–5, Split, Croatia, 2018.

[83] W. Kang, K. Kapitanova, and S. H. Son, "RDDS: a real-time data distribution service for cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 8, pp. 393–405, 2012.

[84] A. Hornsby and R. Walsh, "From instant messaging to cloud computing, an XMPP review," in *IEEE International Symposium on Consumer Electronics (ISCE 2010)*, pp. 1–6, Braunschweig, Germany, 2010.

[85] S. Vinoski, "Advanced message queuing protocol," *IEEE Internet Computing*, vol. 10, pp. 87–89, 2006.

[86] K. Pister and L. Doherty, "TSMP: time synchronized mesh protocol," *IASTED Distributed Sensor Networks*, vol. 391, p. 398, 2008.

[87] R. Seggelmann, M. Tuexen, and M. Williams, "Transport layer security (TLS) and datagram transport layer security (DTLS) heartbeat extension," *Internet Engineering Task Force, RFC*, vol. 6520, 2012.

[88] T. Dreibholz, E. P. Rathgeb, I. Rungeler, R. Seggelmann, M. Tuxen, and R. R. Stewart, "Stream control transmission protocol: past, current, and future standardization activities," *IEEE Communications Magazine*, vol. 49, pp. 82–88, 2011.

[89] B. A. Forouzan, *TCP/IP Protocol Suite*, McGraw-Hill, Inc., 2009.

[90] D. Bandyopadhyay and J. Sen, "Internet of things: applications and challenges in technology and standardization," *Wireless personal communications*, vol. 58, pp. 49–69, 2011.

[91] M. Li, M.-Y. Wu, Y. Li et al., "Shanghai grid as an information service grid: an overview," in *2005 IEEE International Conference on Services Computing (SCC'05) Vol-1*, pp. 351–354, Orlando, FL, USA, 2005.

[92] A. de Saint-Exupery, "Internet of Things," *Strategic Research Roadmap, Corpus ID: 6436852*, 2009.

[93] O. Vermesan and P. Friess, *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*, River Publishers, 2013.

[94] M. A. Alsmirat, F. Al-Alem, M. Al-Ayyoub, Y. Jararweh, and B. Gupta, "Impact of digital fingerprint image quality on the fingerprint recognition accuracy," *Multimedia Tools and Applications*, vol. 78, pp. 3649–3688, 2019.

[95] L. Tan and N. Wang, "Future internet: the internet of things," in *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, pp. V5-376–V5-380, Chengdu, China, 2010.

[96] F. Mattern and C. Floerkemeier, "From the internet of computers to the internet of things," in *From Active Data Management to Event-Based Systems and More*, K. Sachs, I. Petrov, and P. Guerrero, Eds., vol. 6462 of Lecture Notes in Computer Science, pp. 242–259, Springer, Berlin, Heidelberg, 2010.

[97] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (IACAC) for the internet of things," *Journal of Cyber Security and Mobility*, vol. 1, pp. 309–348, 2013.

[98] V. Sharma, R. Kumar, K. Srinivasan, and D. N. K. Jayakody, "Coagulation attacks over networked UAVs: concept, challenges, and research aspects," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 1, pp. 67–72, 2019.

[99] Q. Wen, X. Dong, and R. Zhang, "Application of dynamic variable cipher security certificate in internet of things," in *2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems*, pp. 1062–1066, Hangzhou, China, 2012.

[100] C. Yu, J. Li, X. Li, X. Ren, and B. B. Gupta, "Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer generated hologram," *Multimedia Tools and Applications*, vol. 77, pp. 4585–4608, 2018.

[101] K. Zhao and L. Ge, "A survey on the internet of things security," in *2013 Ninth International Conference on Computational Intelligence and Security*, pp. 663–667, Emeishan, China, 2013.

[102] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," *Computer*, vol. 44, no. 9, pp. 51–58, 2011.

[103] T. Alexenko, M. Jenne, S. D. Roy, and W. Zeng, "Cross-site request forgery: attack and defense," in *2010 7th IEEE Consumer Communications and Networking Conference*, pp. 1-2, Las Vegas, NV, USA, 2010.

[104] S. Li, L. Da Xu, and S. Zhao, "5G internet of things: a survey," *Journal of Industrial Information Integration*, vol. 10, pp. 1–9, 2018.

[105] F. Li and P. Xiong, "Practical secure communication for integrating wireless sensor networks into the internet of things," *IEEE Sensors Journal*, vol. 13, pp. 3677–3684, 2013.

[106] B. V. Sundaram, M. Ramnath, M. Prasanth, and V. Sundaram, "Encryption and Hash based security in internet of things," in *2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN)*, pp. 1–6, Chennai, India, 2015.

[107] R. H. Weber, "Internet of things—new security and privacy challenges," *Computer Law & Security Review*, vol. 26, pp. 23–30, 2010.

[108] Z. Li, X. Yin, Z. Geng et al., "Research on PKI-like protocol for the internet of things," in *2013 Fifth International Conference on Measuring Technology and Mechatronics Automation*, pp. 915–918, Hong Kong, China, 2013.

[109] S. Cirani, G. Ferrari, and L. Veltri, "Enforcing security mechanisms in the IP-based internet of things: an algorithmic overview," *Algorithms*, vol. 6, pp. 197–226, 2013.

[110] E. Hammer-Lahav, D. Recordon, and D. Hardt, "The oauth 1.0 protocol," RFC 5849, 2010.

[111] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, "A survey of lightweight-cryptography implementations," *IEEE Design & Test of Computers*, vol. 24, pp. 522–533, 2007.

[112] S. Ravi, A. Raghunathan, P. Kocher, and S. Hattangady, "Security in embedded systems: design challenges," *ACM Transactions on Embedded Computing Systems*, vol. 3, pp. 461–491, 2004.

[113] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, "Proposed embedded security framework for internet of things (IoT)," in *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)*, pp. 1–5, Chennai, India, 2011.

[114] S. Horrow and A. Sardana, "Identity management framework for cloud based internet of things," in *Proceedings of the First International Conference on Security of Internet of Things—-SecurIT '12*, pp. 200–203, Kollam, India, 2012.

[115] H. Abie and I. Balasingham, "Risk-based adaptive security for smart IoT in eHealth," in *Proceedings of the 7th International Conference on Body Area Networks*, pp. 269–275, Oslo, Norway, 2012.

[116] F. Al Shuhaimi, M. Jose, and A. V. Singh, "Software defined network as solution to overcome security challenges in IoT," in *2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, pp. 491–496, Noida, India, 2016.

[117] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the CONFIDANT protocol," in *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing*, pp. 226–236, Lausanne, Switzerland, 2002.

[118] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Advanced communications and multimedia security*, B. Jerman-Blažič and T. Klobučar, Eds., pp. 107–121, Springer, Boston, MA, 2002.

[119] J. T. Oke, J. Agajo, B. K. Nuhu, J. G. Kolo, and L. Ajao, "Two layers trust-based intrusion prevention system for wireless sensor networks," *Advances inElectrical and Telecommunication Engineering*, vol. 1, pp. 23–29, 2018.

[120] X. Wang, M. Nguyen, J. Carr, L. Cui, and K. Lim, "A group preference-based privacy-preserving POI recommender system," *Information & Communications Technology Express (ICT Express)*, vol. 6, no. 3, pp. 204–208, 2020.

[121] H. Tao and W. Peiran, "Preference-based privacy protection mechanism for the internet of things," in *2010 Third International Symposium on Information Science and Engineering*, pp. 531–534, Shanghai, China, 2010.

[122] C. Bormann, A. P. Castellani, and Z. Shelby, "CoAP: an application protocol for billions of tiny internet nodes," *IEEE Internet Computing*, vol. 16, pp. 62–67, 2012.

[123] K. Gupta and S. Shukla, "Internet of things: security challenges for next generation networks," in *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)*, pp. 315–318, Greater Noida, India, 2016.

[124] N. Gyory and M. Chuah, "IoTOne: integrated platform for heterogeneous IoT devices," in *2017 International Conference on Computing, Networking and Communications (ICNC)*, pp. 783–787, Silicon Valley, CA, USA, 2017.

[125] A. Sarma, A. Matos, J. Girão, and R. L. Aguiar, "Virtual identity framework for telecom infrastructures," *Wireless Personal Communications*, vol. 45, pp. 521–543, 2008.

[126] C. Hu, J. Zhang, and Q. Wen, "An identity-based personal location system with protected privacy in IoT," in *2011 4th IEEE International Conference on Broadband Network and Multimedia Technology*, pp. 192–195, Shenzen, China, 2011.

[127] V. Sharma, I. You, K. Yim, R. Chen, and J.-H. Cho, "BRIoT: behavior rule specification-based misbehavior detection for IoT-embedded cyber-physical systems," *IEEE Access*, vol. 7, pp. 118556–118580, 2019.

[128] D. P. Joseph and J. Norman, "An analysis of digital forensics in cyber security," in *First International Conference on Artificial Intelligence and Cognitive Computing*, R. Bapi, K. Rao, and M. Prasad, Eds., vol. 815 of Advances in Intelligent Systems and Computing, pp. 701–708, Springer, Singapore, 2019.

[129] M. Rogers, "The role of criminal profiling in the computer forensics process," *Computers & Security*, vol. 22, pp. 292–298, 2003.

[130] I. You, K. Yim, V. Sharma, G. Choudhary, R. Chen, and J.-H. Cho, "On IoT misbehavior detection in cyber physical systems," in *2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC)*, pp. 189-190, Taipei, Taiwan, 2018.

[131] S. Alabdulsalam, K. Schaefer, T. Kechadi, and N.-A. Le-Khac, "Internet of things forensics—challenges and a case study," in *Advances in Digital Forensics XIV. Digital Forensics 2018*, vol. 532 of IFIP Advances in Information and Communication Technology, Springer, Cham.

[132] I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. M. A. Kazmi, and C. S. Hong, "Internet of things forensics: recent advances, taxonomy, requirements, and open challenges," *Future Generation Computer Systems*, vol. 92, pp. 265–275, 2019.

[133] Q. Do, B. Martini, and K.-K. R. Choo, "Cyber-physical systems information gathering: a smart home case study," *Computer Networks*, vol. 138, pp. 1–12, 2018.

[134] E. Oriwoh and P. Sant, "The forensics edge management system: a concept and design," in *2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing*, pp. 544–550, Vietri sul Mare, Italy, 2013.

[135] E. Oriwoh and G. Williams, "Internet of things: the argument for smart forensics," in *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance*, IGI-Global Publishing, 2014.

[136] A. Goudbeek, K.-K. R. Choo, and N.-A. Le-Khac, "A forensic investigation framework for smart home environment," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pp. 1446–1451, New York, NY, USA, 2018.

[137] D. Li, L. Deng, B. B. Gupta, H. Wang, and C. Choi, "A novel CNN based security guaranteed image watermarking generation scenario for smart city applications," *Information Sciences*, vol. 479, pp. 432–447, 2019.

[138] M. S. Obaidat, I. Traore, and I. Woungang, *Biometric-Based Physical and Cybersecurity Systems*, Springer, 2019.

[139] I. You, K. Yim, V. Sharma, G. Choudhary, I.-R. Chen, and J.-H. Cho, "Misbehavior detection of embedded IoT devices in medical cyber physical systems," in *Proceedings of the 2018 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies*, pp. 88–93, Washington DC, 2018.

[140] F. Al-Turjman and A. Malekloo, "Smart parking in IoT-enabled cities: a survey," *Sustainable Cities and Society*, vol. 49, p. 101608, 2019.

[141] M. M. Hossain, R. Hasan, and S. Zawoad, "Trust-IoV: a trustworthy forensic investigation framework for the internet of vehicles (IoV)," in *2017 IEEE International Congress on Internet of Things (ICIOT),*, pp. 25–32, Honolulu, HI, USA, 2017.

[142] V. Sharma, I. You, K. Andersson, F. Palmieri, M. H. Rehmani, and J. Lim, "Security, privacy and trust for smart mobile-internet of things (M-IoT): a survey," *IEEE Access*, vol. 8, pp. 167123–167163, 2020.

[143] X. Feng, E. S. Dawam, and S. Amin, "A new digital forensics model of smart city automated vehicles," in *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 274–279, Exeter, UK, 2017.

[144] D. R. Clark, C. Meffert, I. Baggili, and F. Breitinger, "DROP (DRone Open source Parser) your drone: forensic analysis of the DJI Phantom III," *Digital Investigation*, vol. 22, pp. S3–S14, 2017.

[145] Y.-Y. Teing, A. Dehghantanha, K.-K. R. Choo, and L. T. Yang, "Forensic investigation of P2P cloud storage services and backbone for IoT networks: BitTorrent Sync as a case study," *Computers & Electrical Engineering*, vol. 58, pp. 350–363, 2017.

[146] V. Sharma, R. Kumar, and P. Patiala, "Service-oriented middleware for multi-UAV guided ad hoc networks," *IT CoNvergence PRActice (INPRA)*, vol. 2, pp. 24–33, 2014.

[147] V. Sharma, I. You, J. T. Seo, and M. Guizani, "Secure and reliable resource allocation and caching in aerial-terrestrial cloud networks (ATCNs)," *IEEE Access*, vol. 7, pp. 13867–13881, 2019.

[148] T. Heckmann, K. Markantonakis, D. Naccache, and T. Souvignet, "Forensic smartphone analysis using adhesives: transplantation of package on package components," *Digital Investigation*, vol. 26, pp. 29–39, 2018.

[149] H. Abie, "Cognitive cybersecurity for CPS-IoT enabled healthcare ecosystems," in *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)*, pp. 1–6, Oslo, Norway, 2019.

[150] A. Cook, M. Robinson, M. A. Ferrag et al., "Internet of cloud: security and privacy issues," in *Cloud Computing for Optimization: Foundations, Applications, and Challenges*, B. Mishra, H. Das, S. Dehuri, and A. Jagadev, Eds., vol. 39 of Studies in Big Data, pp. 271–301, Springer, Cham, 2018.

[151] G. M. Insights, *Digital Health Market Share Trends 2019–2025 Growth Forecast Report*, Global Market Insights, Selbyville, 2019.

[152] A. McIntyre, B. Blau, and M. Reitz, *Forecast: wearable electronic devices, worldwide*, Gartner, Stamford, CT, USA, 2016.

[153] S. Watson and A. Dehghantanha, "Digital forensics: the missing piece of the internet of things promise," *Computer Fraud & Security*, vol. 2016, pp. 5–8, 2016.

[154] J. Boucher and N.-A. Le-Khac, "Forensic framework to identify local vs synced artefacts," *Digital Investigation*, vol. 24, pp. S68–S75, 2018.

[155] A. Case and G. G. Richard III, "Memory forensics: the path forward," *Digital Investigation*, vol. 20, pp. 23–33, 2017.

[156] D. Quick and K.-K. R. Choo, "IoT device forensics and data reduction," *IEEE Access*, vol. 6, pp. 47566–47574, 2018.

[157] A. Nieto, R. Roman, and J. Lopez, "Digital witness: safeguarding digital evidence by using secure architectures in personal devices," *IEEE Network*, vol. 30, pp. 34–41, 2016.

[158] H. Chung, J. Park, and S. Lee, "Digital forensic approaches for Amazon Alexa ecosystem," *Digital Investigation*, vol. 22, pp. S15–S25, 2017.

[159] M. M. Hossain, R. Hasan, and S. Zawoad, "Probe-IoT: a public digital ledger based forensic investigation framework for IoT," in *INFOCOM Workshops*, pp. 1-2, Birmingham, USA, 2018.

[160] A. Nieto, R. Rios, and J. Lopez, "A methodology for privacy-aware IoT-forensics," in *2017 IEEE Trustcom/BigDataSE/ICESS*, pp. 626–633, Sydney, NSW, Australia, 2017.

[161] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, "Internet of things forensics: challenges and approaches," in *9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, pp. 608–615, Austin, TX, USA, 2013.

[162] L. Perlepes, G. Stamoulis, and P. Kikiras, *An End-to-End Framework for Securing the Internet of Things*, 2011.

[163] S. Perumal, N. M. Norwawi, and V. Raman, "Internet of things (IoT) digital forensic investigation model: top-down forensic approach methodology," in *2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC)*, pp. 19–23, Sierre, Switzerland, 2015.

[164] S. Zawoad and R. Hasan, "Faiot: towards building a forensics aware eco system for the internet of things," in *2015 IEEE International Conference on Services Computing*, pp. 279–284, New york, NY, USA, 2015.

[165] D. Lillis, B. Becker, T. O'Sullivan, and M. Scanlon, "Current challenges and future research areas for digital forensic investigation," 2016, https://arxiv.org/abs/1604.03850.

[166] A. Bijalwan, M. Wazid, E. S. Pilli, and R. C. Joshi, "Forensics of random-UDP flooding attacks," *Journal of Networks*, vol. 10, p. 287, 2015.

[167] V. Sharma, I. You, and G. Kul, "Socializing drones for inter-service operability in ultra-dense wireless networks using blockchain," in *Proceedings of the 2017 International Workshop on Managing Insider Security Threats*, pp. 81–84, Dallas Texas, USA, 2017.

[168] V. Arora, R. S. Leekha, K. Lee, and A. Kataria, "Facilitating user authorization from imbalanced data logs of credit cards using artificial intelligence," *Mobile Information Systems*, vol. 2020, Article ID 8885269, 13 pages, 2020.

[169] T. G. Zewdie and A. Girma, "IOT security and the role of AI/ML to combat emerging cyber threats in cloud computing environment," *Issues in Information Systems*, vol. 21, no. 4, pp. 253–263, 2020.

[170] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[171] J. Pacheco, V. H. Benitez, and Z. Pan, "Security framework for IoT end nodes with neural networks," *International Journal of Machine Learning and Computing*, vol. 9, pp. 381–386, 2019.

[172] E. Hodo, X. Bellekens, A. Hamilton et al., "Threat analysis of IoT networks using artificial neural network intrusion detection system," in *2016 International Symposium on Networks, Computers and Communications (ISNCC)*, pp. 1–6, Yasmine Hammamet, Tunisia, 2016.

[173] A. Mishra, N. Gupta, and B. Gupta, "Defense mechanisms against DDoS attack based on entropy in SDN-cloud using POX controller," *Telecommunication Systems*, pp. 1–16, 2021.

[174] A. Dahiya and B. B. Gupta, "A reputation score policy and Bayesian game theory based incentivized mechanism for DDoS attacks mitigation and cyber defense," *Future Generation Computer Systems*, vol. 117, pp. 193–204, 2021.

[175] C. Esposito, M. Ficco, and B. B. Gupta, "Blockchain-based authentication and authorization for smart city applications," *Information Processing & Management*, vol. 58, article 102468, 2021.

[176] B. Dickson, "How blockchain can change the future of IoT," *Venture Beat*, vol. 20, 2016.

[177] V. Sharma, J. Kim, S. Kwon, I. You, and F.-Y. Leu, "An overview of 802.21a-2012 and its incorporation into IoT-fog networks using osmotic framework," in *International Conference on Internet of Things as a Service*, pp. 64–72, Taichun, Taiwan, 2017.

[178] V. Sharma, I. You, F. Palmieri, D. N. K. Jayakody, and J. Li, "Secure and energy-efficient handover in fog networks using blockchain-based DMM," *IEEE Communications Magazine*, vol. 56, pp. 22–31, 2018.

[179] V. Sharma, J. D. Lim, J. N. Kim, and I. You, "SACA: self-aware communication architecture for iot using mobile fog servers," *Mobile Information Systems*, vol. 2017, Article ID 3273917, 17 pages, 2017.

[180] M. Alrowaily and Z. Lu, "Secure edge computing in IoT systems: review and case studies," in *2018 IEEE/ACM Symposium on Edge Computing (SEC)*, pp. 440–444, Seattle, WA, USA, 2018.

[181] Y. Li and S. Wang, "An energy-aware edge server placement algorithm in mobile edge computing," in *2018 IEEE International Conference on Edge Computing (EDGE)*, pp. 66–73, San Francisco, CA, USA, 2018.

[182] E. Oyekanlu, C. Nelatury, A. O. Fatade, O. Alaba, and O. Abass, "Edge computing for industrial IoT and the smart grid: channel capacity for M2M communication over the power line," in *2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON)*, pp. 1–11, Owerri, Nigeria, 2017.

[183] V. Sharma, I. You, D. N. K. Jayakody, D. G. Reina, and K.-K. R. Choo, "Neural-blockchain-based ultrareliable caching for edge-enabled UAV networks," *IEEE Transactions on Industrial Informatics*, vol. 15, pp. 5723–5736, 2019.

[184] J. Gill, I. Okere, H. HaddadPajouh, and A. Dehghantanha, "Mobile forensics: a bibliometric analysis," in *Cyber Threat Intelligence*, A. Dehghantanha, M. Conti, and T. Dargahi, Eds., vol. 70 of Advances in Information Security, pp. 297–310, Springer, Cham, 2018.

[185] Y. Y. Teing, A. Dehghantanha, and K. K. R. Choo, "CloudMe forensics: a case of big data forensic investigation," *Concurrency and Computation: Practice and Experience*, vol. 30, article e4277, 2018.

[186] I. Yaqoob, E. Ahmed, I. A. T. Hashem et al., "Internet of things architecture: recent advances, taxonomy, requirements, and open challenges," *IEEE wireless communications*, vol. 24, pp. 10–16, 2017.

[187] Z. Li, V. Sharma, and S. P. Mohanty, "Preserving data privacy via federated learning: challenges and solutions," *IEEE Consumer Electronics Magazine*, vol. 9, pp. 8–16, 2020.

[188] A. Nieto, R. Rios, and J. Lopez, "IoT-forensics meets privacy: towards cooperative digital investigations," *Sensors*, vol. 18, p. 492, 2018.

[189] A. Nieto, R. Rios, and J. Lopez, "Digital witness and privacy in IoT: anonymous witnessing approach," in *2017 IEEE Trustcom/BigDataSE/ICESS*, pp. 642–649, Sydney, NSW, 2017.

[190] V. Sharma, J. Kim, S. Kwon, I. You, K. Lee, and K. Yim, "A framework for mitigating zero-day attacks in IoT," 2018, https://arxiv.org/abs/1804.05549.

[191] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: the case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 618–623, Kona, HI, USA, 2017.

[192] V. Sharma, I. You, and N. Guizani, "Security of 5G-V2X: technologies, standardization and research directions," *IEEE Network*, vol. 34, no. 5, pp. 306–314, 2020.

[193] O. Gupta, S. Rani, and D. C. Pant, "Impact of parallel computing on bioinformatics algorithms," in *Proceedings 5th IEEE International Conference on Advanced Computing and Communication Technologies*, pp. 206–209, Rohtak, Haryana, India, 2011.

[194] R. Alharbi and D. Aspinall, "An IoT analysis framework: an investigation of IoT smart cameras' vulnerabilities," in *Living in the Internet of Things: Cybersecurity of the IoT—2018*, London, UK, 2018.

[195] M. A. Zamora-Izquierdo, J. Santa, J. A. Martínez, V. Martínez, and A. F. Skarmeta, "Smart farming IoT platform based on edge and cloud computing," *Biosystems engineering*, vol. 177, pp. 4–17, 2019.

[196] R. Singh, A. Gehlot, J. K. Khilrani, and M. Mittal, "Internet of things-triggered and power-efficient smart pedometer algorithm for intelligent wearable devices," in *Wearable and Implantable Medical Devices*, pp. 1–23, Elsevier, 2020.

[197] M. Mittal, S. Tanwar, B. Agarwal, and L. M. Goyal, *Energy Conservation for IoT Devices: Concepts, Paradigms and Solutions*, vol. 206, Springer, 2019.

[198] M. Abdel-Basset, G. Manogaran, and M. Mohamed, "Internet of things (IoT) and its impact on supply chain: a framework for building smart, secure and efficient systems," *Future Generation Computer Systems*, vol. 86, pp. 614–628, 2018.

[199] F. Piccialli and A. Chianese, *Editorial for FGCS Special Issue: The Internet of Cultural Things: Towards a Smart Cultural Heritage*, vol. 81, Elsevier, 2018.

[200] P. Radanliev, D. C. de Roure, R. Nicolescu et al., "Future developments in cyber risk assessment for the internet of things," *Computers in Industry*, vol. 102, pp. 14–22, 2018.

[201] N. H. N. Zulkipli, A. Alenezi, and G. B. Wills, "IoT forensic: bridging the challenges in digital forensic and the internet of things," in *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security*, pp. 315–324, Porto, Portugal, 2017.

[202] M. Husamuddin and M. Qayyum, "Internet of things: a study on security and privacy threats," in *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, pp. 93–97, Abha, 2017.

[203] I. Lee and K. Lee, "The internet of things (IoT): applications, investments, and challenges for enterprises," *Business Horizons*, vol. 58, pp. 431–440, 2015.

[204] M. Babar, A. Rahman, F. Arif, and G. Jeon, "Energy-harvesting based on internet of things and big data analytics for smart health monitoring," *Sustainable Computing: Informatics and Systems*, vol. 20, pp. 155–164, 2018.

[205] J. Liu and W. Sun, "Smart attacks against intelligent wearables in people-centric internet of things," *IEEE Communications Magazine*, vol. 54, pp. 44–49, 2016.

[206] Y. Zhang, R. H. Deng, G. Han, and D. Zheng, "Secure smart health with privacy-aware aggregate authentication and access control in internet of things," *Journal of Network and Computer Applications*, vol. 123, pp. 89–100, 2018.

[207] S. Din and A. Paul, "Retracted: Smart health monitoring and management system: toward autonomous wearable sensing for internet of things using big data analytics," *Future Generation Computer Systems*, vol. 91, pp. 611–619, 2019.

[208] S. S. S. R. Depuru, L. Wang, V. Devabhaktuni, and N. Gudi, "Smart meters for power grid—challenges, issues, advantages and status," in *2011 IEEE/PES Power Systems Conference and Exposition*, pp. 1–7, Phoenix, AZ, USA, 2011.

[209] A. C. Jose and R. Malekian, "Improving smart home security: integrating logical sensing into smart home," *IEEE Sensors Journal*, vol. 17, pp. 4269–4286, 2017.

[210] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in *2012 International Conference on Computer Science and Electronics Engineering*, pp. 648–651, Hangzhou, China, 2012.

[211] S. Vashi, J. Ram, J. Modi, S. Verma, and C. Prakash, "Internet of things (IoT): a vision, architectural elements, and security issues," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pp. 492–496, Palladam, India, 2017.

[212] W. Zhang and B. Qu, "Security architecture of the internet of things oriented to perceptual layer," *International Journal on Computer, Consumer and Control (IJ3C)*, vol. 2, pp. 37–45, 2013.

[213] R. Kumar, H. Sharma, M. Mittal, and P. S. Rana, "Editorial. Wireless sensor network: design, architecture, application, data communication security and management," *International Journal of Sensors Wireless Communications and Control*, vol. 7, pp. 169–169, 2017.

[214] L. Li, S. Li, T. Tryfonas, and H. Li, "The internet of things: a security point of view," *Internet Research*, vol. 26, no. 2, pp. 337–359, 2016.

[215] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "DTLS based security and two-way authentication for the internet of things," *Ad Hoc Networks*, vol. 11, pp. 2710–2723, 2013.

[216] T. G. Robertazzi, "Software-defined networking," in *Introduction to Computer Networking*, pp. 81–87, Springer, 2017.

[217] V. R. Kebande and I. Ray, "A generic digital forensic investigation framework for internet of things (IoT)," in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 356–362, Vienna, Austria, 2016.

[218] M. M. Losavio, K. Chow, A. Koltay, and J. James, "The internet of things and the smart city: legal challenges with digital forensics, privacy, and security," *Security and Privacy*, vol. 1, article e23, 2018.

[219] B. Cavallo, G. Di Crescenzo, D. Kahrobaei, and V. Shpilrain, "Efficient and secure delegation of group exponentiation to a single server," in *International Workshop on Radio Frequency Identification: Security and Privacy Issues*, pp. 156–173, New york, USA, 2015.

[220] L. Li, R. Lu, K.-K. R. Choo, A. Datta, and J. Shao, "Privacy-preserving-outsourced association rule mining on vertically partitioned databases," *IEEE Transactions on Information Forensics and Security*, vol. 11, pp. 1847–1861, 2016.

[221] A. Alrawais, A. Alhothaily, C. Hu, X. Xing, and X. Cheng, "An attribute-based encryption scheme to secure fog communications," *IEEE access*, vol. 5, pp. 9131–9138, 2017.

[222] J. Zhang, Q. Li, X. Wang, B. Feng, and D. Guo, "Towards fast and lightweight spam account detection in mobile social networks through fog computing," *Peer-to-Peer Networking and Applications*, vol. 11, pp. 778–792, 2018.

[223] M. Agrawal and P. Mishra, "A comparative survey on symmetric key encryption techniques," *International Journal on Computer Science and Engineering*, vol. 4, p. 877, 2012.

[224] D. J. Wu, A. Taly, A. Shankar, and D. Boneh, "Privacy, discovery, and authentication for the internet of things," in *Computer Security—ESORICS 2016. ESORICS 2016*, I. Askoxylakis, S. Ioannidis, S. Katsikas, and C. Meadows, Eds., vol. 9879 of Lecture Notes in Computer Science, pp. 301–319, Springer, Cham, 2016.

[225] X. Liang, X. Lin, and X. S. Shen, "Enabling trustworthy service evaluation in service-oriented mobile social networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, pp. 310–320, 2013.

[226] J. Ni, K. Zhang, K. Alharbi, X. Lin, N. Zhang, and X. S. Shen, "Differentially private smart metering with fault tolerance and range-based filtering," *IEEE Transactions on Smart Grid*, vol. 8, pp. 2483–2493, 2017.

[227] S. Salonikias, I. Mavridis, and D. Gritzalis, "Access control issues in utilizing fog computing for transport infrastructure," in *International Conference on Critical Information Infrastructures Security*, pp. 15–26, Berlin, Germany, 2015.

[228] S. Chandrasekhar and M. Singhal, "Efficient and scalable query authentication for cloud-based storage systems with multiple data sources," *IEEE Transactions on Services computing*, vol. 10, pp. 520–533, 2015.

[229] X. Yang, F. Yin, and X. Tang, "A fine-grained and privacy-preserving query scheme for fog computing-enhanced location-based service," *Sensors*, vol. 17, p. 1611, 2017.

[230] G. Zhuo, Q. Jia, L. Guo, M. Li, and P. Li, "Privacy-preserving verifiable data aggregation and analysis for cloud-assisted mobile crowdsourcing," in *IEEE INFOCOM 2016—The 35th Annual IEEE International Conference on Computer Communications*, pp. 1–9, San Francisco, CA, USA, 2016.

[231] IC3, 2020, March 2021, https://www.ic3.gov/.

[232] M. A. Iqbal, O. G. Olaleye, and M. A. Bayoumi, "A review on internet of things (IoT): security and privacy requirements

and the solution approaches," *Global Journal of Computer Science and Technology*, vol. 16, no. 7-E, 2017.

[233] A. Fathy, I. F. Tarrad, H. F. Hamed, and A. I. Awad, "Advanced encryption standard algorithm: issues and implementation aspects," in *International Conference on Advanced Machine Learning Technologies and Applications*, pp. 516–523, Cairo, Egypt, 2012.

[234] Z. Wan, Z. Xu, S. Liu, W. Ni, and S. Ye, "An internet of things roaming authentication protocol based on heterogeneous fusion mechanism," *IEEE Access*, vol. 8, pp. 17663–17672, 2020.

[235] F. Monsen and K. Glisson, *Differencing Engine for Digital Forensics*, 2020, Google Patents.

[236] J. D. McEachron, *Forensic Investigation Tool*, 2019, Google Patents.

[237] M. Morimoto, Y. Shirai, and H. Takeda, *Forensic System, Forensic Method, and Forensic Program*, 2016, Google Patents.

[238] K. SeongKu, J. Mincheol, C. Youngjun, J. Choi, K. SinKyu, and S. Jungtaek, *Device and Method for Providing Security in Remote Digital Forensic Environment*, 2017, Google Patents.

[239] Y. H. Choi, T. G. Kim, H. G. Oh, and D. H. Lee, *Method and Apparatus for Digital Forensics*, 2012, Google Patents.

[240] M. M. Shannon and M. J. Decker, *Systems and Methods for Provisioning Digital Forensics Services Remotely over Public and Private Networks*, 2015, Google Patents.

[241] W. J. Buchanan, J. R. Graves, and N. Bose, *Digital Forensics*, 2014, Google Patents.

[242] Y. H. Gil, J. Y. Lee, S. H. Jo, Y. S. Kim, K. W. Kim, S. S. Lee et al., *Method for Data Analysis and Digital Forensics and System Using the Same*, 2014, Google Patents.

[243] K. L. Levy, *Forensic Digital Watermarking with Variable Orientation and Protocols*, 2008, Google Patents.

[244] T. L. Carpenter and W. J. Westerinen, "Secure digital forensics," 2011, Google Patents.

[245] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *Ieee Access*, vol. 6, pp. 115–124, 2017.

[246] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-based solutions to security and privacy issues in the internet of things," *IEEE Wireless Communications*, vol. 25, pp. 12–18, 2018.

[247] U. Javaid, M. N. Aman, and B. Sikdar, "DrivMan: driving trust management and data sharing in VANETS with blockchain and smart contracts," in *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, pp. 1–5, Kuala Lumpur, Malaysia, 2019.

[248] K. R. Ozyilmaz and A. Yurdakul, "Designing a blockchain-based IoT with Ethereum, swarm, and LoRa: the software solution to create high availability with minimal security risks," *IEEE Consumer Electronics Magazine*, vol. 8, pp. 28–34, 2019.

[249] V. Sharma, "An energy-efficient transaction model for the blockchain-enabled internet of vehicles (IoV)," *IEEE Communications Letters*, vol. 23, pp. 246–249, 2018.

[250] K. Valtanen, J. Backman, and S. Yrjölä, "Blockchain-powered value creation in the 5G and smart grid use cases," *IEEE Access*, vol. 7, pp. 25690–25707, 2019.

[251] U. Javaid, A. K. Siang, M. N. Aman, and B. Sikdar, "Mitigating IoT device based DDoS attacks using blockchain," in *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, pp. 71–76, Munich, Germany, 2018.

[252] O. Novo, "Blockchain meets IoT: an architecture for scalable access management in IoT," *IEEE Internet of Things Journal*, vol. 5, pp. 1184–1195, 2018.

[253] P. Lv, L. Wang, H. Zhu, W. Deng, and L. Gu, "An IoT-oriented privacy-preserving publish/subscribe model over blockchains," *IEEE Access*, vol. 7, pp. 41309–41314, 2019.

[254] U. Javaid, M. N. Aman, and B. Sikdar, "Blockpro: blockchain based data provenance and integrity for secure iot environments," in *Proceedings of the 1st Workshop on Blockchain-Enabled Networked Sensor Systems*, pp. 13–18, Shenzhen, China, 2018.