ISSN 2347 - 3983

Volume 8. No. 9, September 2020

International Journal of Emerging Trends in Engineering Research

Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter254892020.pdf

https://doi.org/10.30534/ijeter/2020/254892020

Internet of Things (IoT) Characteristics, Applications, and Digital Forensics Investigation Process: A Review

Deepti Rani[1, 2], **Nasib Singh Gill**[3]

[1]Research Scholar, Department of Computer Science & Applications,
Maharshi Dayanand University, Rohtak, Haryana (India)
[2]Assistant Professor, Chandigarh University, Mohali, Punjab (India)
[3]Professor, Department of Computer Science & Applications,
Maharshi Dayanand University, Rohtak, Haryana (India)
[1, 2]deepti.sindhu@gmail.com,[3]nasibsgill@gmail.com

ABSTRACT

In the present era, the requirement of machine to machine communication is increasing very rapidly. Internet of Things (IoT) is creating abundant opportunities in business, government, education, and health. IoT is gaining popularity in many other areas too with the reduction in cost of smart computing technologies. Now building a network of all kinds of devices and objects has become possible after emergence of sensors, actuators, transducers, and embedded system. Data flows through various entities using wireless sensor networks and IoT systems. The entire machine to machine (M2M) communication interface can use any communication protocol (such as Bluetooth, 3G, 4G, Z-Wave, Wi-Fi, NFC, LTE, Ethernet, LoRaWAN, Radio, Cellular, and etc.). Objects can be sensed and controlled across any network infrastructure in digital environment using IoT technology. Physical world is being integrated into computer based digital systems resulting which the benefit of less human intervention. Now human is living into cyber-physical world where performed operations are more accurate, efficient and economic. Connected devices used in different environments present many opportunities as well as risks in front of cyber-physical world. These risks or incidents could be identified using digital forensics investigation technology. Hence, digital forensics must be properly explored for solving various malicious problems of IoT. This paper presents a survey of the need of digital forensics in ongoing IoT applications. Various threats faced by IoT enabled smart environment also have been discussed in the present paper. Paper also highlights some applications, characteristics, and application criteria of IoT in digital domain. The main objective of this paper is to present general process phases of digital forensics. One more motive of this paper is to identify and explore various reasons to deploy digital forensics in IoT enabled smart environment in different application domains.

Key words: Internet of Things (IoT); Digital Forensics; Digital Forensics Investigation Process.

1. INTRODUCTION

Internet of Things (IoT) concept was first inaugurated in 1999 after the big explosion of wireless devices and with the origination of some technologies like Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSN) [1]. Usage of IoT devices and Services is increasing abruptly for last many decades. Sensors and communicating devices are integrated with IoT system resulting which the smart objects have become capable to communicate with each other without human intervention. These smart nodes function autonomously and can interact with any connected node (object) anytime, anywhere. Some functions of these integrated systems are: delivery of data, accessing cloud based resources, data extraction, data gathering and data analysis for making decisions. IoT is a merged system of digital machines, people, and electronic or mechanical objects which are provided with unique identifiers and having a potential of data transferring over a network. IoT enabled devices are being exploited in all inclusive application domains like smart healthcare system, business intelligence system, smart railway and traffic signaling system, smart monitoring, smart metering system, and above all smart home and smart city. Today, data is coming exponentially as the result of actions performed by smart IoT devices [2].

IoT has increased business opportunities in last many years. Surrounding devices are dependent upon cloud infrastructure and IoT services (data access, data storage, data transfer and data analysis) offered by cloud [3]. Data associated with IoT applications is stored in cloud and can be retrieved easily for investigation of digital offences [4].

Though IoT enabled devices offer large amount of services which have changed human life but it has created many security concerns too. Several vulnerabilities and security risks are arising throughout the secure data communication, data privacy and data storage process. Many cyber attacks come with this connectedness and have become significant challenges for IoT enabled smart environment. IoT is creating unusual opportunities for hackers and cyber criminals [5]. Data and IoT devices of educational organizations, business organizations, and industrial organizations on national and international level are the major targets of numerous threats and incidents [6]. IoT devices and services are growing very rapidly and technology has exposed to vulnerability and insecure network connection that leads to serious cyber attacks. For making IoT environment and its network more strong and secure, special tools and techniques are needed to be deployed. More efficient forensic mechanisms must be designed and implemented for analysis and investigation [2].

Forensic experts use standard digital forensic frameworks and models for forensics analysis and investigation [4]. Traces are accumulated from crime related devices and networks to study crime related incidents followed by recreation [7]. Initially, these works were proposed for crime investigation in IoT industries. There are countless challenges as well as usefulness of IoT devices which are impacting people's daily life. Most of the devices used in IoT enabled smart environment have been designed without focusing on strong security measures which enable it to accommodate various kinds of threats [8], [9]. There is a great usefulness of traces in investigation of offences. The traces could be accessed using forensic tools and devices from any smart application domain (e.g. smart home), but obtaining only meaningful data is a big challenge [10]. Many smart phone applications and interfaces have been developed for extraction and analysis of digital traces in order to discover security vulnerabilities and threats [11]. Sensors and actuators used in IoT devices generate amount of data which may be useful for digital forensics. Digital traces may be categorized according to certain measuring attributes like pressure, temperature, location, movement, presence, time, distance, calories burnt in walk, and so on; depending upon the application. The traces could be extracted from associated devices like smart-phones, computers, laptops, or smart automated devices. Traces for investigation could also be extracted from multiple sources including network, memory and application software. Sometimes the traces could be endangered by cyber criminals. Hence, it is important to preserve all digital traces and must be stored with proper security.

2. INTERNET OF THINGS

IoT is a comprehensive technology. This technology enables small devices to perform as smart devices. Such devices communicate with each other using different types of network media, software, hardware, tools and mechanisms. Though these are ordinary devices but after getting Internet connection, these ordinary devices become uniquely identifiable, contactable and addressable. The communication results enable sensors to return appropriate actions. The main aim of IoT is to make human life dynamic and easy. IoT is used in regular applications; some examples of which are: automatic car drive, smart light on and off, door locking-unlocking, air conditioning according to room temperature, giving alert by intelligent refrigerator and many more [12], [13]. Health monitoring is one of the best applications of IoT system. This system can remotely monitor various activities of human body and gather information like heart beat, blood pressure, pulse rate, oxygen rate, and temperature using some specific sensors [14], [15]. Communications like machine-to-machine, man-to-machine, machine-to-man, and man-to-man are possible using IoT technology. Some devices do have server functionality and also can respond readily to different incoming requests. But some very less sophisticated devices can only generate output and transmit on some triggers [16]. Power sources may also vary. Some IoT devices take power from main supply while some other devices like low-power battery operated devices having limited lifespan may take power from self generating supply.

2.1 Internet of Things (IoT) Characteristics

So far, many characteristics have been discovered and defined by IoT experts. All these characteristics cover the definition of IoT system. Fig. 1 shows some key and general characteristics of IoT system which have been identified during many research studies [4], [13], [17], and [18].

- **Things:** Anything or any object that has been designed to be connected can probably become the part of the IoT system. Such things are connected and tagged through Internet and contain certain important parts like sensors, actuators, and networking features.
- **Data:** Data is the first element towards Internet of Things that works as connector to join all things, actions and intelligence.
- **Intelligence:** IoT is not a single technology. It comes with many other technologies, algorithms, software, hardware, computational systems and their combinations. These all facts provide intelligent spark and make a thing smart.
- **Connectivity:** Many devices are connected through single or multiple networks. This can also be called M2M or machine to machine network. Connectivity provides accessibility and compatibility to a network.
- **Sensing:** Sensors come up with the ability to sense and understand the physical world. This technology helps in creating experiences for awareness of physical world. Sensors simply take some input and provide a rich and great understanding.
- **Ecosystem:** It is place where IoT makes a platform for other technologies, communities and goals. Here one more dimension is provided that is named as 'Internet of Everything (IoE)'.

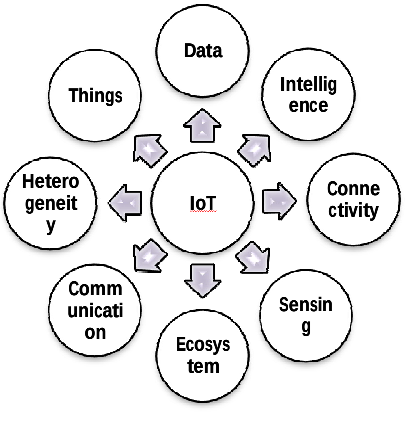

Figure 1: Internet of Things (IoT) Characteristics

- **Communication:** Devices get connected to each other in order to communicate data. The communicated data may be analyzed. Various network technologies are used for data communication.
- **Heterogeneity:** Different objects connected in IoT infrastructure use different hardware, software, and network platforms and communicate with each other very efficiently.

2.2 Internet of Things (IoT) Applications

IoT has been promoted to be used in different application areas. IoT was first termed in supply chain management in 1999 by Kevin Asthon [19], [20]. Along with the time, significantly more smart devices have been connected to the Internet. IoT European Research Cluster (IERC) has represented classification of some relevant application areas of smart healthcare [12], [21]. Today none of the application domain remains untouched from the facilities given by IoT. It is not easy to enlist all the application areas which are supported by IoT (directly or indirectly). But we present some very popular applications of IoT which have changed human life abruptly [13]-[15], [22], [23]:

- Supply Chain Management
- Remote Health Monitoring, diagnosis, and treatment
- Environment Monitoring and Sensing
- Agriculture Applications
- Weather Forecasting System
- Habitat Monitoring System
- Underwater Monitoring and Management
- Surveillance Cameras (Traffic, Home, Business)
- Smart Home System
- Traffic Management System
- Smart Transportation
- Smart Parking
- Industrial Automation System
- Smart Wearable
- Smart Cities
- Smart Grid
- Inventory Management System
- Safety, Security and Risk Management
- Quality Control and Management
- Connected Cars
- Smart Retail Management and etc.

3. DIGITAL FORENSICS

Digital forensics act as the most important security component in IoT enabled smart environment. Digital forensics is a technique that is used for bridging various security challenges which come in the path of IoT [17]. Before 2006, there was no separate law in U.S. federation for electronically stored information (ESI) to be treated as evidence in the civil cases. After revision, in 2006 the scope of evidence was broadened by Federal Rules of Civil Procedure (FRCP). Law enforcement agencies and civil courts started including digital information in the digital category of evidence. Discovered data may be stored in hard drives, VM logs or RAM. The investigation of digital or computer based crimes gave rise to new specialized technology known as computing forensics [24].

3.1 Definition of Digital Forensic Science

According to a definition given by Palmer "Digital forensic science is the use of scientifically derived and proven methods toward evidence preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidences which are obtained from digital sources in order to facilitate or furthering the adaptation or reconstruction of events to find related criminal(s), or helping to predict unauthorized actions shown to be disruptive to planned operations." (Palmer, 2001: 16) [25].

3.2 Digital Forensics Investigation Process

Crime investigation is the primary activity that is started with complete survey of crime scene. Crime scene is surveyed by forensic experts in order to gather all related evidences and proceed for crime investigation. Digital evidences are preserved and scanned to obtain relevant information supporting investigation. Although various forensics models and frameworks have been proposed so far for different digital environments [26]; still there is lack of universal standardization. Here we will discuss only certain general and widely used processes of digital forensics investigation which are considered by maximum forensic experts in different countries [27]-[29]. Fig. 2 shows general digital forensics investigation processes.

Forensic Readiness phase: This phase shows the preparedness of digital forensic investigation. This is pre-incident phase which is used before crime identification. In fig. 2, Forensic readiness phase has been shown in dotted lines because this is an optional phase. Digital Forensic Readiness will be discussed in detail later in the next sub-section [30].

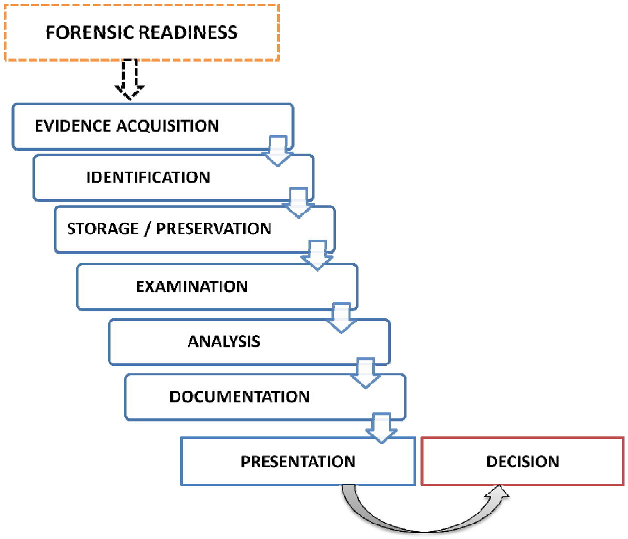

Figure 2: Digital Forensics Investigation Processes

Evidence acquisition phase: All the evidences like assets and objects present on crime scene are acquired before starting the investigation. Evidences could be physical or digital or both. Physical evidences are collected on the basis of fingerprints, footprints, blood samples or other pieces of traces. Potential digital evidences are acquired under e-discovery by seizing and securing electronic devices which can generate evidences [30]. Before considering any digital traces as the key evidences, it must be assured that those should not be tempered with. Digital evidences may be in the form of useful digital files, folders, images, and/or clips on storage media of computers and it may be in form of videos or pictures in camera, CCTV footage, data generated by sensors. Evidences in the form of text messages, voice calls and social media accounts could be traced from mobile phones of victim or suspects [31].

Identification phase: Acquisition phase is followed by identification phase. Relevant and potential digital information is identified from the amount of acquired evidences. There is one main difference between acquisition phase and identification phase. In the acquisition phase all possible evidences are obtained from crime scene while in identification phase, the most important information is assessed that may become useful for case solving [32].

Storage or Preservation phase: It is very important to safely preserve the identified digital evidences. Criminal can temper with or alter the evidences in case of any negligence. Physical and digital, both types of securities of digital evidences are equally important. Useful information must be preserved carefully in encrypted form in reliable storage devices at a safe place. The information must be kept fully confidential. It must not be allowed to be accessed by unauthorized people and must be secured from vulnerabilities. Existing guidelines related to security must be properly followed [31].

Examination phase: All physical and digital examination must take place properly in specialized laboratories by forensic experts [33]. Latest forensic tools, software and hardware must be used in order to get progressive results on examination of collected data. Collected digital evidences must be reliable, complete, authentic, believable, and admissible [34].

Analysis phase: In analysis phase, evidences are linked to find the cause of incident. Findings are reviewed to confirm the identity of the criminal. The results of examination must be analyzed in order to draw conclusions. The analyzed information must be effective and efficient enough to answer the questions related to the crime [35].

Documentation phase: All evidence related reports are documented to present in cyber court of law [36]. Analyzed data should be properly documented in acceptable format. Reports, files or templates may be created based on analyzed data.

Presentation/ Reporting phase: NIST describes this phase as the process which contains description of performed actions [34]. The prepared documents must be immediately presented in cyber court of law in form of report or any acceptable format. Delay in presentation might affect the whole investigation process. Criminal may temper with the documented evidences even before presentation, if presentation delayed. Due to this, wrong or false testimony might be presented in front of judiciary which may derive injustice. Evidence presentation process is accomplished in two main steps: analysis presentation and analysis proving [Kohn]. Hence, the confidentiality and integrity of evidences must be preserved till the end of the case [7].

Decision phase: Finally, the decision is drawn on the basis of presented documents, reports, videos, pictures, witnesses and examined evidences.

Forensic investigators also conduct possible interrogations to victims or connected people to obtain important information. Subsequent activities like restrictions of any physical or electronic object on crime scene are performed in order to maintain integrity. All possible evidences are identified, collected, labeled and documented and then sent to laboratory. Specialized computers, toolkits and software must be used for conducting all investigation activities. Digital evidences need to be handled very carefully because improper handling may cause changes in evidence and lose of originality. Variety of tools and methodologies are available in the world of digital forensics for investigation. Contended reports must be documented, stored and kept available for further review.

3.3 Digital Forensic Readiness (DFR)

Forensic Readiness may be defined as the potential of an organization to scrutinize with maximum potential and maximum cost. This is the preparedness of an organization to become able to collect, store, analyze and present evidences in order to use in much effective way. There are various functional requirements for the readiness of adding digital forensics in IoT [30]. Every electronic device used by criminal certainly leaves some traces behind, which are associated with user’s activities. These traces could be treated as evidences which can prove the facts of cyber incident. DFR is mainly used in business environments and industries to deal with security risks. DFR also guarantees the security of IoT enabled smart environment. But only few devices in different organizations are prepared to handle security risks. Devices used in IoT environments must be configured securely, patched carefully against vulnerabilities, and monitored and updated frequently.

In [37], Jason described the implementation of DFR by approaching a pro-active process in order to increase the operational efficiency in business organizations. He also described in his work that how proper evidence collection, preservation and presentation can impact digital crimes, incidents and threats. Reddy and Venter in [38], proposed some necessary concepts for DFR Management System targeting an optimal level of DFR for business organizations.

ISO/IEC has presented DFR-IoT architecture in a good way including detailed Forensic Investigation process workflow for digital infrastructures. Digital forensic readiness processes complies with ISO/IEC 27043: 2015 standard [29]. DFR-IoT architecture includes three major key components: Proactive process, IoT communication mechanism, and Reactive process. Fig. 3 shows the key components of DFR-IoT..

Digital Forensic Readiness comprises of proactive process measures. Proactive process provides guidelines and techniques before crime identification or may be before happening of the crime [39]. Forensic Readiness is deployed in Government, academic and other organizational areas in all over the world.

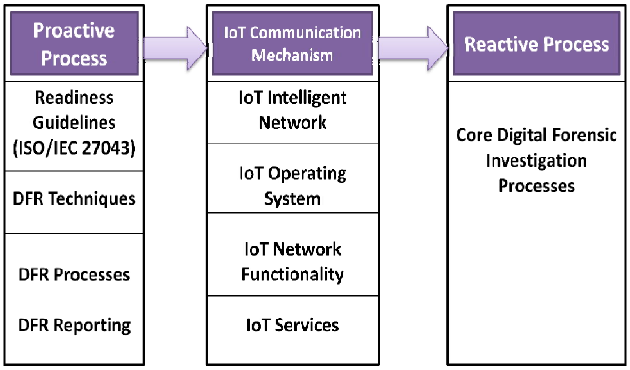
Proactive Process
Readiness Guidelines (ISO/IEC 27043)
DFR Techniques
DFR Processes
DFR Reporting
IoT Communication Mechanism
IoT Intelligent Network
IoT Operating System
IoT Network Functionality
IoT Services
Reactive Process
Core Digital Forensic Investigation Processes

Figure 3: Digital Forensic Readiness-IoT Architecture [29]

The main objective of forensic readiness is pre-incidental security [40]. Sometimes organizations have to face difficulties while implementation of digital forensic readiness which may effect forensic investigations in specific application domains [41]. Proactive measures need to be undertaken to deal with cybercrimes efficiently in the organizations.

4. NEED OF DIGITAL FORENSICS IN IOT

As the usage of IoT technology is increasing, cyber/digital crime incidents are also increasing day by day. Thousands of such major cases have been reported so far in cyber court of law. One of such cases is Internet Threat Security Symantec's [17]. Many more such attacks have been detected and reported which are: Ransomware, SQL Injection, Phishing attacks, Man-in-middle attack [42], fraud and other malicious attacks. Cyber crimes are also committed through IoT devices and IoT applications. IoT devices process, store and produce amount of data in digital form; so these devices have been proved as goldmine of data for attackers [43]. Now days, cyber attackers are taking advantage of COVID-19. Most of the people are connected to Internet. Throughout the world, smart devices are connected to each other through RFID, wireless sensor network (WSN) and Internetwork. Whole public and private data is transported through these networks. Hackers can easily attack on communicated data and commit any form of offence. Criminals can check into machines and attack via Email, messages, and phones. COVID-19 is giving opportunities to cyber criminals. Malware, phishing, smishing, and social engineering are some popular growing attacks through which people's machines and devices are being targeted in this pandemic outbreak.

Digital forensics techniques are used for detection of cyber crimes, identification of related evidences and suspects to dig out crime cause and offender's information. Traditional forensic techniques are not sufficient for investigation in IoT enabled smart environment. Crimes in IoT environment are very much different from ordinary crimes. Hence, some real time investigation processes are needed. Some new emerging approaches have been proposed for investigation purposes so far for smart environment [17].

4.1 Need of Digital Forensics in IoT Enabled Smart Environment

In this section some cases have been discussed which prove digital forensics as an important necessity for cyber crime investigation [44], [45]. It has been discussed earlier that IoT devices do process and store amount of data in various smart environments. Criminal can spy on every personal detail on user's device. On some browsers, any opened page may host malicious code. This data may present risks as well as opportunities for forensic viewpoint. These devices also produce traces which can be useful for forensic and investigative purposes. In addition, the evidence traces may also present evaluation challenges even for forensic experts [11]. Here are some examples of smart environment in which necessity of digital forensics has been shown for several purposes [46]:

- **Evidence Identification, Collection and preservation from Heterogeneous Environments and Data Heterogeneity:** Connected devices in different IoT environments generate different forms of data. Any form of data need to be transformed into digital form for getting processed and stored. Identification of relevant evidences is the primary objective of any investigation procedure. All evidences need to be collected and preserved for crime investigation. Ordinary forensics is not sufficient to handle such crime investigation. When any digital crime needs to be identified; in most of the cases no proper forensically sound documented method or reliable tool persists to collect evidences [47]. Using traditional techniques, only collected data could be preserved. But preservation of the crime scene and real-time evidence is an immense challenge [43]. Digital forensics may be considered as a suitable solution.

- **Security of Data in IoT Devices:** Different types of devices in IoT environment may be connected to each other or to some other electronic devices using networks and sensors. But in both cases some data is transferred over the network. This data may be attacked or stolen by cyber criminals. Cyber criminals can control the sensors used in devices, wearable, body suits, medical services, tablets and mobile phones. According to Science Daily news, criminals can crack security PIN by just tracking the motion of user's mobile phone or device. Malicious attackers may also attack on user's gadgets just by downloading apps and opening websites [48]. Many of them do not need to ask for permission to access user's devices while some are accessed by user's permission. Knowingly or unknowingly user allow for the access permission [49]. In some cases, it becomes worse when user closes the device completely, still hacker attacks on the secret information of the user. Security of information could be achieved by monitoring devices against attackers. Criminals related to such crime can be identified using digital forensics.

- **Protection of IoT Devices:** IoT devices produce massive amounts of data. There are several concerns related to privacy and security. Here major concern may be about devices; means how much they are protected against threats. The protection may also be analyzed using digital forensics. Password protected devices may be hacked by stealing the PIN [48].

- **Security of Smart Application Domains:** Digital forensics is also useful in smart homes, smart cities and smart organizational environments to identify, trace, store and analyze suspected data. These realistic smart environments are equipped with large numbers of smart devices with variety of applications. Devices and applications which are currently used in smart environments can be trapped into security threats. For instance; smoke detectors used in homes and offices could be disabled that can cause fire incident [49]. Smart door locks could be locked or unlocked by attackers for harming the user. Further, variety of such problems can be created by controlling different type of sensors (temperature, pressure, proximity, light, smoke and etc.) used in different smart environments. Most of the latest smart applications are provided with forensics capability.

- **Security of Smart Transportation:** Digital Forensics plays an important role in transport management system. Different countries have designed their administrative structures based on international laws. Although these structures are based on the international standards but still reflects the flexibility and suitability for their people. Digital forensics laws have been adopted in each national transportation management system to avoid various cyber crimes. Michael et al compared legal regimes of many countries in different smart environments including smart transportation system. Authors in [50] also discussed various transportation and parking issues. Threats in smart transportation cause many risks like road accidents, traffic congestion, airplane crash, street light failure, lack of discipline. Cyber criminals may divert traffic on road and airways by controlling traffic signals. Street and road lights may also be controlled. Brakes, door-locks or other parts of smart vehicles may be failed by hacking into the system. These risks result in loss of life and other damages. Digital Forensics system controls these risks by risk identification.

5. CONCLUSION

After reviewing various researches it has been concluded that security is the primary obstacle in the way of successful deployment of IoT in different application domains. Normal security solutions are not adequate for solving so many problems of different nature in dynamic IoT environment. Paper summarizes so many other problems which are rich of challenges. Digital forensics is used for incident identification and reconstruction by evidence collection, analysis, preservation, and presentation in court of law. The present paper highlights the general phases of digital forensic investigation processes. The paper also summarizes the basic functional requirements for digital forensics readiness (DFR). In the present paper authors also identify and explore various purposes of digital forensics and some reasons to deploy digital forensics in IoT enabled smart environment in different application domains.

REFERENCES

[1] I. T.Union, **ITU Internet Reports 2005: The Internet of Things**, 2015. http://www.itu.int/osg/spu/publications/internetofthings/ [Last accessed: 28 August, 2020].

[2] U. Karabiyik and K. Akkaya. **Digital Forensics for IoT and WSNs**. Mission-Oriented Sensor Networks and Systems, November 2018, pp.1-42.

[3] F. Jamal and Dr. R. Zaman Khan. **Emerging Technologies and Developments in Cloud Computing: A Systematic Review.** International Journal of Emerging Trends in Engineering Research, vol. 8, no. 3, March 2020, pp. 894-905.

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

[5] J. McGehee, D. Spofford, and M. Haan. **What Engineering Leaders Need to Know About IoT Security**. a white paper, Very, 2020, pp. 1-15.

[6] X. Jiang, M. Lora, and S. Chattopadhyay. **An Experimental Analysis of Security Vulnerabilities in Industrial IoT Devices**, ACM Trans. Internet Technol., vol. 1, no. 1, January 2020, pp. 1-24.

[7] S. Zawoad and R. Hasan. **FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things**, in *IEEE International Conference on Services Computing*, New York, 2015, pp. 279-284.

[8] H. F. Atlam, A. Alenezi, M. O. Alassafi, A. A. Alshdadi and G. B. Wills. **Security, Cybercrime and Digital Forensics for IoT.** InPeng SL., Pal S., Huang L. (eds) Chapter 22, Principles of Internet of Things (IoT), Springer, Cham, January 2020, pp. 551-577.

[9] M. Parvez M, R. S. E. Ravindran, S. Inthiyaz, Ch. Tejkumar, K. Veera, R. Sai, K. A. S. Reddy. **Network Security using Notable Cryptographic Algorithm for IoT Data.** vol. 8, no. 5, May 2020, 2169-2172.

[10] S. Kim, M. Park, S. Lee, and J. Kim. **Smart Home Forensics—Data Analysis of IoT Devices**, Electronics, vol. 9, issue 1215, 2020, pp. 1-13.

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

[12] Z. Kamal, A. Mohammed and E. S. Ali Ahmed. **Internet of Things Applications, Challenges and Related Future Technologies**, World Scientific News, vol. 67, no. 2, 2017, pp. 126-148.

[13] K. K. Patel and S. M. Patel. **Internet of Things-IoT: Definition, Characteristics, Architecture, Enabling**

Technologies, Application & Future Challenges. International Journal of Engg Sc. and Computing, vol. 6, no. 5, pp. 529-551, May 2016.

[14] S. M. Thaung, H. M. Tun, K. K. Win, M. Than. **Exploratory Data Analysis Based on Remote Health Care Monitoring System by Using IoT**. Communications, vol. 8, issue 1, 2020, pp. 1-8.

[15] R. R. Chintala, Ch N. S. M. Akhilesh , N. P. P. Ganesh, T. Ravideep. **Wireless Sensor Network for m-Healthcare Monitoring of Human Being.** vol. 8, no. 5, May 2020, pp. 1685-1688.

[16] R. C. Hegarty, D. J. Lamb and A. Attwood. **Digital Evidence Challenges in the Internet of Things,** Chapter 2 – WDFIA Papers, pp. 163-172.

[17] N. H. NikZulkipli, A. Alenezi and G. Wills. **IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things.** 2nd International Conf. on Internet of Things, Big Data and Security (IoTBDS), vol. 1, Jan 2017, pp. 315-324.

[18] i-SCOOP (**The Internet of Things (IoT) – essential IoT business guide**). https://www.i-scoop.eu/internet-of-things/ [Last accessed: 5 September, 2020].

[19] Postscapes-Tech, **Internet of Things (IoT) History** https://www.postscapes.com/iot-history/ [Last accessed: 28 August, 2020].

[20] K. Ashton. That **Internet of Things** Thing. RFID Journal, vol. 22, no. 7, 2009, pp. 97-114.

[21] Z. Alansari, S. Soomro, M. R. Belgaum and S. Shamshirband. **The Rise of Internet of Things (IoT) in Big Healthcare Data: Review and Open Research Issues.** Progress in Advanced Computing and Intelligent Engineering, Advances in Intelligent Systems and Computing, vol. 564, January 2018, pp. 675-685.

[22] S. Singh, I. Chana, and R. Buyya. **Agri-Info: Cloud Based Autonomic System for Delivering Agriculture as a Service**. Internet of Things, vol. 9, 2020, pp. 1-16.

[23] H. F. Atlam and Gary B. Wills. **IoT Security, Privacy, Safety and Ethics.** July 2019, pp. 123-149.

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

[25] G. Palmer. **A Road Map for Digital Forensic Research**. Technical Report (DTRT0010-01) for First Digital Forensic Research Workshop (DFRWS), New York, 2001.

[26] J. Hou, Y. Li, J. Yu, and W. Shi. **A Survey on Digital Forensics in Internet of Things**. IEEE Internet of Things Journal (Volume: 7 , Issue: 1 , Jan. 2020, pp. 1-15.

[27] N. Kishore, C. Gupta and D. Dawar. **An Insight View of Digital Forensics.** International Journal on Computational Sciences & Applications (IJCSA), vol.4, no. 6, December 2014, pp. 89-96.

[28] I. Kigwana, V. R. Kebande, H. S Venter. **A Proposed Digital Forensic Investigation Framework for an eGovernment Structure for Uganda**, IST-Africa Conference May 2017, pp.1-8.

[29] ISO/IEC 27043: 2015 (EN). Information technology -- Security techniques - Incident investigation principles and processes. https://www.iso.org/obp/ui/#iso:std:iso-iec:27043:ed-1:v1:en [Online-Accessed at:

[30] V. R Kebande, N. M Karie and H S Venter. **Adding Digital Forensic Readiness as a Security Component to the IoT Domain**. International Journal on Advanced Science, Engineering and Information Technology, vol. 8, no. 1, 2018, pp. 1-11.

[31] A. Valjarevic and H. S. Venter. **A Comprehensive and Harmonized Digital Forensic Investigation Process Model**. Journal Of Forensic Sciences, vol. 60, no. 6, 2015, pp. 1467-1483.

[32] S. Zawoad and R. Hasan. **FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things**. 12th IEEE International Conference on Services Computing (SCC), June 27- July 2, 2015, pp. 279-284.

[33] N. Beebe and J. Clark. **A Hierarchical, Objectives-Based Framework for the Digital Investigations Process**. DFRWS, vol. 2, no. 2, 2004, pp. 147-167.

[34] H. Jahankhani and J. Ibarra. **Digital Forensic Investigation for the Internet of Medical Things (IoMT).** HSOA Journal of Forensic, Legal & Investigative Sciences, vol. 5, issue 2, 2019.

[35] M. Kohn, M. S. Olivier, and J. H. P. Eloff. **Framework for a Digital Forensic Investigation**. Proceedings of the ISSA 2006 from Insight to Foresight Conference, 5-7 July, 2006, pp. 1-8.

[36] S. Subektiningsih, Y. Prayudi and I. Riadi. **Digital Forensics Workflow as A Mapping Model for People, Evidence, and Process in Digital Investigation**. International Journal of Cyber-Security and Digital Forensics (IJCSDF), vol. 7, no. 3, 2018, pp. 294-304.

[37] S. Jason. **Implementing Digital Forensic Readiness: From Reactiveto Proactive Process.** 1st Edition. EBook ISBN: 9780128045015. Copyright: © Syngress 2016.

[38] K. Reddy, and H. S. Venter. **The architecture of a digital forensic readiness management system**. Computers & security, vol. 32, Feb. 2013, pp. 73-89.

[39] S. Alharbi, J. Weber-Jahnke, and I. Traore. **The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review**. International Journal of Security and its Applications, vol. 5, no. 4, 2011, pp. 59-71.

[40] A. Mouhtaropoulos, C-T. Li and M. Grobler. **Digital Forensic Readiness: Are We There Yet?** Journal of International Commercial Law and Technology, vol. 9, no.3, 2014, pp. 173-179.

[41] N. M. Karie and S. M. Karume. **Digital Forensic Readiness in Organizations: Issues and Challenges**. Journal of Digital Forensics, Security and Law, vol. 12, no. 4, article 5, December 2017, pp. 43-54.

[42] H. Mohapatra, S. Rath, S. Panda, R. Kumar. **Handling of Man-In-The-Middle Attack in WSN Through Intrusion Detection System**. International Journal of Emerging Trends in Engineering Research, vol. 8, no. 5, May 2020, pp. 1503- 1510.

[43] M. Conti, A. Dehghantanha, K. Franke, S. Watson. **Internet of Things Security and Forensics: Challenges and Opportunities.** July 2017, pp. 544-546.

[44] E. Oriwoh, D. Jazani and G. Epiphaniou. **Internet of things forensics: challenges and approaches**. In: 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, 2013, pp. 608-615.

[45] S. Khan. **The Role of Forensics in the Internet of Things: Motivations and Requirements**. In Proc. IEEE Internet Initiative eNewsletter, July 2017.

[46] T. Zia, P. Liu and W. Han. **Application-Specific Digital Forensics Investigative Model in Internet of Things (IoT).** ARES '17: Proceedings of the 12th International Conference on Availability, Reliability and Security, vol. 55, 2017, pp. 1-7.

[47] C. J. D'Orazio, K. R. Choo and L. T. Yang. **Data Exfiltration From Internet of Things Devices: iOS Devices as Case Studies**. In Proc. IEEE Internet of Things Journal, vol. 4, no. 2, April 2017, pp. 524-535.

[48] Science News Article, **Are your sensors spying on you?**, Newcastle University, 11 April, 2017. https://www.sciencedaily.com/releases/2017/04/170411085825.htm [Last Accessed on: 29 August, 2020].

[49] M. Mehrnezhad, E. Toreini, S. F. Shahandashti, F. Hao. **Stealing PINs via mobile sensors: actual risk versus user perception**, International Journal of Information Security, vol. 17, no. 3, 2018, pp 291-313.

[50] M. M. Losavio, K. P. Chow, A. Koltay and J. James. **The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy and security**. John Wiley and Sons Ltd., 26 April 2018, pp. 1-11.