Fog Forensics: A Comprehensive Review of Forensic Models for Fog Computing Environment

Konrad Śniatała, Yashas Hariprasad, K. J. Latesh Kumar, Naveen Kumar Chaudhary, and Michał Weissenberg

Abstract Numerous potential social advantages are offered by fog computing, including personalized healthcare, smart cities, agri technology, automated transportation, consumer IoT, and many more. Ambient computing at previously unfathomable scales is made possible by the extremely dynamic and complex nature of fog computing and its low latency communication networks connecting sensors, devices, and actuators. The need to look for digital forensic methods that may effectively be used to solve computer-related crimes utilizing IoT devices is being driven by the rise in IoT devices. Fog computing adds greater threats to privacy and security as it is becoming challenging given the increasing number of linked devices. The existing forensics models are not sufficient to handle data from the fog cloud. In this paper, we present a thorough review of the existing state-of-the-art forensic models that can be applied to fog cloud environment and this work can further be used to promote extensive research and development of fog forensic models.

Keywords Fog computing · Digital forensics · IoT · Privacy and security

K. Śniatała (✉) · M. Weissenberg
Poznan University of Technology, Poznan, Poland
e-mail: konrad.sniatala@doctorate.put.poznan.pl

M. Weissenberg
e-mail: michal.weissenberg@put.poznan.pl

Y. Hariprasad · K. J. Latesh Kumar
Florida International University, Miami, FL 33174, USA
e-mail: yhari001@fiu.edu

K. J. Latesh Kumar
e-mail: lkumarkj@fiu.edu

N. K. Chaudhary
National Forensics Sciences University, Gandhinagar, Gujarat, India
e-mail: naveen.chaudhary@nfsu.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2024

S. J. Patel et al. (eds.), *Information Security, Privacy and Digital Forensics*,
Lecture Notes in Electrical Engineering 1075,
https://doi.org/10.1007/978-981-99-5091-1_3

1 Introduction

1.1 Fog Versus Cloud Computing

In recent years, an enormous increase in the amount of devices connected to the Internet has been observed. According to [1], currently, the amount of IoT appliances having access to the web in 2022 reached 14.4 billion and is predicted to increase by 2025 to 27 billion.

So far, the most popular used solution to process data is based on cloud computing. As defined by NIST (National Institute of Standards and Technology), cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [2]. Consequently, cloud computing can be understood as resources available online (usually as a service) by a third party. The most popular example of cloud computing is web file storage and management (e.g., Google Drive, Dropbox, and AWS). In this model, data collected on a device (e.g., smartphone, surveillance camera, temperature sensor, etc.), is sent via the Internet to a remote server located far away. In industrial applications, data in various formats, which are generated by IoT devices and sensors, are then transferred to remote cloud services (e.g., AWS or Microsoft Azure). Next, the information is processed and the results are sent back to the source device. Unfortunately, this solution could encounter many issues and limitations due to the unstable internet connection, security, bandwidth limit, and latency. However, not all data generated by the sensors needs to be sent immediately to the cloud. There are many cases where latency is critical for the system and the response is needed in real time (e.g., autonomous cars, emergency power cut sensors, etc.). In such cases, the processing needs to happen faster, then the time it takes to send data to a cloud server and receive an answer.

In order to outcome these limitations, fog computing has been introduced. The term "fog computing" has been used initially by Cisco, and is sometimes used interchangeably (incorrectly) with "edge computing". Fog and edge are two different and separate layers. Fog is a layer placed between cloud and end (edge) devices. Fog computing devices receive data directly from the sensors. They process them, do the filtering, and return the result directly to the edge resource. Obviously, data can still be sent to the cloud, but this process does not have to be applied with each request. Information can be aggregated and sent to cloud less often for archiving or further analyses. Fog computing was introduced as an alternative to widely used "cloud computing", but at the same time being complimentary. The main difference distinguishing these two approaches is data storage and processing location. In fog computing, a remote cloud is usually not used to store large amount of data. Instead, information is being kept in a more decentralized location, which is way closer to the source of the data (device which generates it).

Thanks to the reduced distance, all data transfer processes can be accomplished locally, which is much less complex. Fog computing layer (Fig. 1) can be compared to

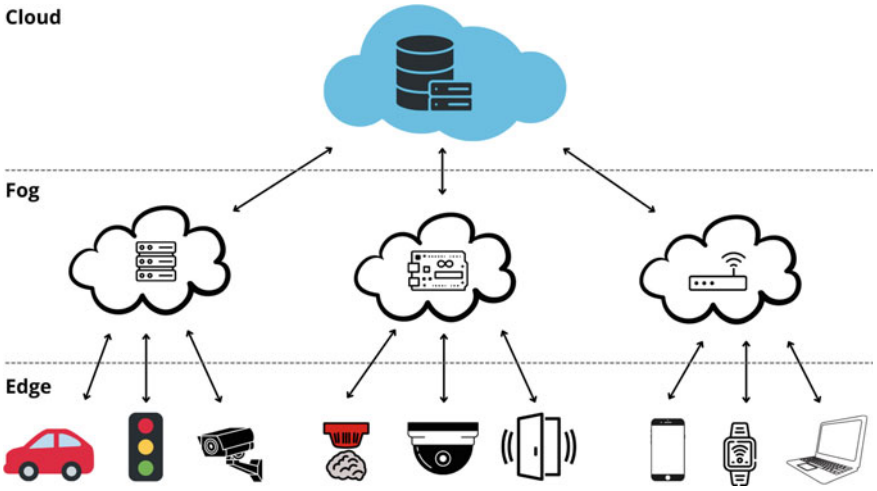

Fig. 1 Cloud, fog, and edge computing layers

a mediator between the edge device and the cloud. Such a solution makes transferring data using fog computing infrastructure quicker and much more efficient compared to the "traditional" cloud computing model.

Fog computing is widely used in a wide range of systems like road traffic control, air quality monitoring, waste management, and many others.

1.2 Digital IoT Forensics

These years due to the emerging amount of small portable devices, being able to connect to the Internet, cybersecurity and digital forensics are disciplines, which evolve extremely fast. Internet of Things (IoT) can be defined as an environment/system of interconnected and interrelated computing devices. IoT devices use technologies such as machine-to-machine communication, context-aware computing, or radio-frequency identification (RFID). Due to exchanging data with devices all around the world, IoT appliances have become a target for hackers, who try to expose the transmitted and stored information. According to [3], in 2021, there have been over 1 billion IoT attacks conducted, from which nearly 900 million were IoT-related phishing attacks. If an attack is successful and data is stolen, tampered, or encrypted, digital forensic specialists are in charge to trace the attacker. Digital forensics can be defined as the process of identification, preservation, analysis, documentation, and presentation (Fig. 2) of the results from digital evidence. This order of digital evidence processing has to be preserved to be officially accepted in a court. Following this scheme also reduces the opportunity for criminals to tamper with the evidence [4]. During many years, special tools have been developed to help and assist forensic

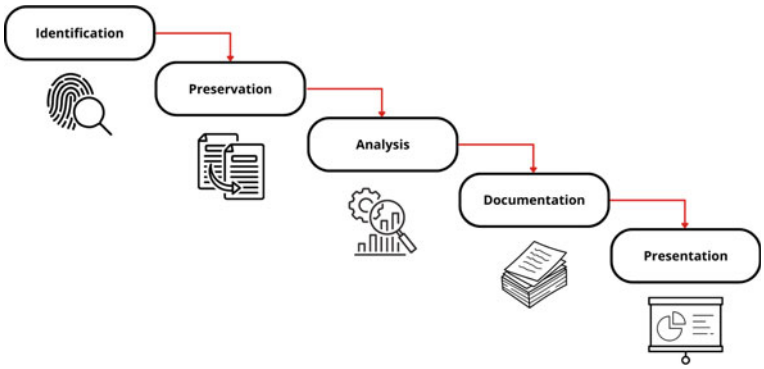

Fig. 2 Digital forensics process

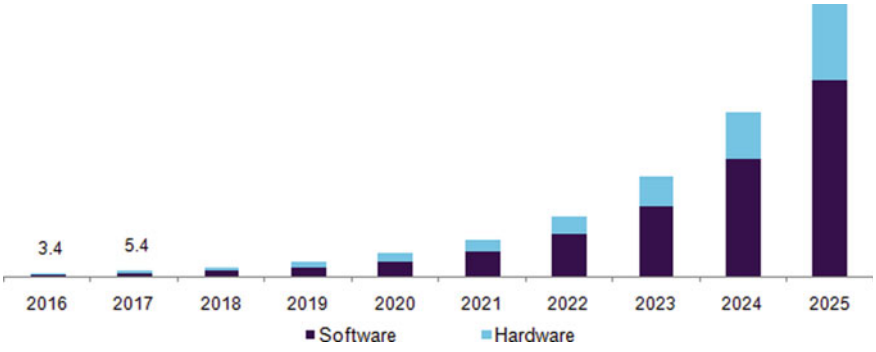

Fig. 3 US fog computing market

investigators with capturing, analyzing, and preserving the most valuable information.

IoT devices are most widely used in the fog computing environment. Due to this fact, the need to look for digital forensic methods that may effectively be used to solve computer-related crimes utilizing IoT devices is being researched.

Researchers are estimating that fog computing market is going to grow exponentially in the next 5 years as shown in Fig. 3. According to the authors, we can see the multi-fold growth only in the United States [5]. Considering the growth globally, we can estimate that the cyber attacks on fog computing would also grow at the same rate and we would need to have robust digital forensics methods and processes to handle the large number of forensics request that may be coming in to the law enforcement agencies.

In this paper, we present a thorough review of the existing state-of-the-art forensic models that can be applied to the fog cloud environment and this work can further be used to promote extensive research and development of fog forensic models.

2 Fog Forensics—Literature Survey

Nowadays, more and more cybercrime investigators, use digital forensics methods in order to solve cases. Big amount of data and the state-of-the-art technology used by criminals make conducting the analysis extremely challenging. The field of fog computing is a layer rich in data and information, which can be crucial to solving cases. Unfortunately, at the same time, diversity of available technology and various platforms, where fog computing can be applied, make it difficult to define universal forensic models for fog computing.

The authors in [6] investigate the methodological, technological, legal, and geopolitical challenges associated with digital forensic investigations in fog computing. The authors present a comprehensive review of the areas that require greater investigations. A framework to stimulate further consideration and discussion regarding the challenges associated with extracting digital evidence from fog computing systems is also presented in the article. This paper gives a clear understanding about the areas that need more concentration and development of intelligent technologies and digital forensics methods required in those areas to tackle the increasing number of cyber attacks.

Authors of [7] have reviewed various fog computing forensic methods. They have put most focus on Advanced Persistent Threat (APT) attacks. APT attacks are usually conducted by whole campaigns (group of hackers), who target military, government, or financial institutions in order to steal high sensitive data. According to [8], 2.8 billion malware attacks were recorded in the first half of 2022 and a sharp 77% rise in IoT malware and a 132% leap in encrypted threats sent via HTTPS. Taking into account the amount of cybersecurity attacks conducted so far in 2022 is highly possible that an organization or individual is going to be sooner or later targeted with a cyberattack and its data might be compromised. In order to gain knowledge and ways of conducting APT attacks aforementioned authors of [7], have proposed a method to implement an enhanced particle swarm optimization PSO algorithm. It is designed for detecting APT attack infections and studying their spread across the fog environment. As the authors describe, their aim is to develop a new approach in order to "Integrate Cyber Threat Intelligence with Digital Forensics analysis in a proactive security approach." Such a solution will open possibilities to detect the APT attacks in the cloud and fog environment before they reach the destination environment. Afterward, data types affected by the APT attack and their prevalence behavior could be analyzed. Another APT attack was studied in [9]. Researchers analyzed Shamoon malware in fog computing using FPSO (Frequency Particles Swarm Optimization) based on the Travelling Salesman approach (TSP). The proposed system (experiment) consisted of the following steps [9]:

1. Fog nodes initialization (three data types: industrial, medical, and educational).
2. Creation of Shamoon attack—followed by distance matrix evaluation. Attack focuses on industrial data.
3. FPSO parameters initialization, along with particle function evaluation.
4. Finding the shortest path (nearest neighborhood).

5. Detecting local best and global best solutions.

Researchers evaluated the performance of the proposed system and observed attack distribution of Shamoon data. As a result, the authors [9] proposed a threat intelligence scheme for analysis and investigative behavior of Shamoon attacks spread (fog computing edges).

As fog computing is executed mostly on small processing units, many researchers covered in their works and papers IoT Fog Forensics. These days modern cars are equipped with multiple small computers and sensors. Fog computing is useful within vehicular processing. As presented in [10], such solution enhances the communication efficiency and overcomes multiple limitations such as latency or real-time response. The mentioned factors and relevant in terms of autonomous cars, where decisions based on multiple sensor data have to be made immediately. End fog processing nodes can be located at the end of vehicular networks. Thanks to such solution they can acquire, process, and store traffic and in-vehicle parameters in real time.

According to [11], a typical modern car has the power computing of 20 personal computers. The software contains over 100 million lines of code and with the use of over 100 sensors collects over 25GB of data per hour. Significantly, higher values appear when taking into consideration autonomous vehicles. As presented in [12], during autonomous test drives, a car can generate on average up to 20 TB of data a day. When a test drive is performed with a more advanced sensor set, this number can increase even to up to 100 TB/day. Such big amount of data is caused by multiple parameters measured by modern vehicles, e.g., location (GPS coordinates), performance (velocity, RPM), and physical parameters (G-force), usually several times per second [13]. It is worth mentioning that sensors, which provide data to the processing units are not always 100% reliable. If a sensor is faulty, the reliability is compromised. The authors of [14] proposed a hybrid algorithm which is designed to solve problem by making proper decision, even if some of the input data is faulty.

Such a big amount of data established various security and forensic challenges in vehicular fog computing. Unfortunately, the awareness of potential threats and mitigating risks in the field of vehicular fog forensics is at a very low level. According to [10], attacks directed in vehicular fog computing (VFC) systems can be categorized into passive and active. Attacks may be conducted by an external (without the knowledge of key computing components) or internal attacker, who is equipped with information originating from compromised fog nodes or other smart vehicles. Passive attacks aim at compromising private information stored in the car systems, whereas active attacks try to interrupt properly functioning VFC systems. As presented by the authors of [10], a secure VFC system implementation should have the following features: confidentiality, integrity, authentication, access control, non-repudiation, availability, reliability, and forensics. The purpose of forensics is to ensure fog nodes data collection, identification, and analysis in order to trace and compromise the source of attack. Most of the forementioned requirements can be fulfilled by applying various encryption techniques, but this only protects the VFC system from passive attacks—aimed to steal data. Unfortunately, in order to detect fog nodes compromises, more elaborate forensic techniques need to be applied. The

authors of [10] analyzed an attack to compromise fog nodes in a fog-assisted traffic control system. Afterward, in order to increase security, they proposed fog forensic models as countermeasures for attackers. The first and most important step is to identify the compromised fog nodes, without disturbing the performance of the functioning system. A solution, the use of evidence-based digital forensic approach combined with traffic-based analysis approach based on real-time and historical traffic data has been proposed in [10]. Evidence-based digital forensic approach focuses on smart vehicle data and (possibly) compromised fog node artifact analysis. In this approach, the authors prepared a traffic simulation, with smart vehicles having probabilities to properly identify compromised nodes or mistakenly badly mark proper nodes. Unfortunately, due to data noise generated by the smart vehicles, it is hard to detect compromised nodes. The second fog forensic analysis approach uses deep learning algorithms and big data analysis. Information from a compromised node, which usually differs from normal data, could be identified and downloaded from cloud servers containing historical and archive evidence. Relation between the fog nodes can be examined to identify the compromised nodes based on the real-time traffic changes [10]. Described solutions, combined with other approaches [15, 16] for detecting abnormalities in traffic network, show how challenging in terms of forensics this topic is. Authors of [17] have even proposed a dynamic traffic congestion management algorithm. It was based on social interactions between vehicles and commuters—Social Internet of Vehicles (SIoV) concept.

Fog computing processing is usually completed on IoT devices, which play a major role in three main domains: Society, Environment, and Industry. As presented in [18], the field of medicine and health care is a part of the society domain. Thanks to the high response time, low latency, and real-time data processing, fog processing takes healthcare applications to the next level. In the following paper [19], the authors have presented a systematic literature review of fog computing technologies in healthcare IoT systems. Researchers have reviewed a total of nearly 100 articles. Only papers on fog computing in healthcare applications have been included in the review. Results were divided into three major classes; frameworks and models, systems (implemented or architecture), and review and survey.

As presented in [19], patients' vital sign monitoring is one of the most important aspect in healthcare systems [20]. This is the reason many researchers focus on exploring and enhancing data collection solutions. An interesting example of a fog-based monitoring system was presented by the authors of [21]. They proposed a secure "Health Fog" framework of where fog computing was used as a layer between the cloud and the end users. In order to enhance privacy and security, additional cloud access security broker was implemented within the solution. As presented in [22], fog computing has the ability to handle a variety of devices and sensors in addition to provide local processing and storage. According to [19], fog computing is the most suitable technique for healthcare IoT systems, which due to the importance and highly sensitive data, require specific features. Mostly used solutions in healthcare IoT systems (based on cloud computing) cannot withstand excessive demands of healthcare systems like reliability, processing speed, or energy awareness.

In addition, a very important aspect concerning the analysis of systems with distributed data sources connected via fog computing is precision and accuracy, which is very difficult to maintain due to the distributed structure and the emerging noise in the system. Many sensor fusion algorithms can be found in the literature, which can help to determine the precision of the system. The paper [23] presents several approaches to information fusion such as Byzantine agreement, Marzullo's interval-based approach, and the Brooks–Iyengar fusion algorithm. Furthermore, the article [24] presents an information fusion approach for blockchain. Ensuring precision at an appropriate level is also crucial from the point of view of system security and the possibility of detecting potential attacks that affect precisely the precision.

As commonly known devices within fog computing environment might contain important data related to criminal activity, essential for forensic investigations. In the work [25], the author has conducted different experiments with fog networks and evaluated existing digital forensic frameworks for IoT fog devices. Research and testing were done in a specially prepared simulated fog environment. Such an approach gave the possibility to observe the way in which the dynamic service movement can affect the evidence location and nodes data storage possibilities. Conducted experiments were aimed to check the usability of digital forensic methods with IoT fog devices. Author of [25] prepared three scenarios of possible attacks on an IoT fog device:

1. Surveillance camera that captured footage of a criminal activity. This device was placed within a fog network.
2. IoT device located within fog network was infected with malware and further used as a part of a botnet attack.
3. IoT device located within a large-scale fog network, contained sensitive data. A criminal found and stole this data.

In the research paper [25], the author tested multiple frameworks implemented to help investigators with the forensic process. Scenario type and network scale significantly affected the applicability of the tested frameworks. The third case with the most large-scale and complex network, was the scenario where all of the tested frameworks were relevant give. In the first case, which differed from the two others, tested frameworks would not give any significant results. On the other hand, in this example due to the smaller network, it is easier to locate and identify the infected node. As stated by [25], usually specific frameworks focusing on fog IoT are aimed at detecting abnormalities in the network and stopping further incidents, which might not be applicable in all fog-based IoT networks.

The forensics methods that are currently employed by law enforcement agencies are not befitting the collection of evidence about an attack involving IoT and fog systems [26]. To bridge this gap, authors introduced "FoBI: fog-based IoT forensic framework" which is suitable for IoT systems which produce and handle large amount of data and when a large number of devices are deployed. The authors propose to filter the data that requires transmission and to obtain the evidence based on the interaction of the devices. Once the model detects an unusual activity, it alerts the

devices of potential threat. By doing this, an attack on all the other devices can be prevented and will not be propagated to the other connected devices.

The authors present two use cases to demonstrate the proposed model: Smart Refrigerator Use Case and Smart City Network of Sensors.

An interesting and comprehensive work, concerning fog computing privacy and security has been presented in [27]. Authors have marked two main fog computing privacy and security challenges: "Proximity of the fog nodes" and "Stringent requirements in fog computing". A malicious attack, which later has to be analyzed using forensic methods, is a significant threat in the fog computing environment. According to the authors [27], these attacks can be categorized as follows:

- Attacks against the Network infrastructure (Denial of Service, Man-in-the-middle, and Rogue gateway).
- Attacks against the edge data center (Data leakage, Privilege escalation, Service manipulation, and Rogue data center).
- Attacks against the core infrastructure (Illegal data access, Service manipulation, and Rogue infrastructure).
- Attacks against virtualization infrastructure (Denial of Service, Misuse of resources, Data leakage, Privilege escalation, and VM manipulation).
- Attacks launched by user devices (Data injection and Service manipulation).
- Web-based attacks.
- Malware-based attacks.

In order to protect the devices and defend such attacks, it is required to apply certain countermeasures, e.g., secure the API and apply policy enforcement access mechanisms or intrusion detection systems. The authors [27] have also discussed the cross-border issues and fog forensics. It has been proven that fog forensic challenges are more difficult compared to cloud forensics. As an example, collecting logged data from the numerous fog network devices is way harder than getting data from, a cloud computing server (Fig. 4).

As stated in [27] fog forensics needs international legislation and jurisdictions in order to try to unify the forensic models, which could be used on fog computing devices.

Extracting digital evidence from fog architecture is a time-consuming and very challenging task. The most important difficulties are mentioned in the following points:

1. various manufacturers—fog layer devices are manufactured by different companies. Although there are some common communication protocols, many manufacturers equip their devices with unique systems. In such cases, forensic investigators need to initially analyze the operating systems in order to get access and download data.
2. data formats—some devices save data in specific unpopular formats or structures. This lack of standardization makes the information more secure and safe, but on the other hand, requires more complex and sophisticated forensic expert solutions and approaches to extract it.

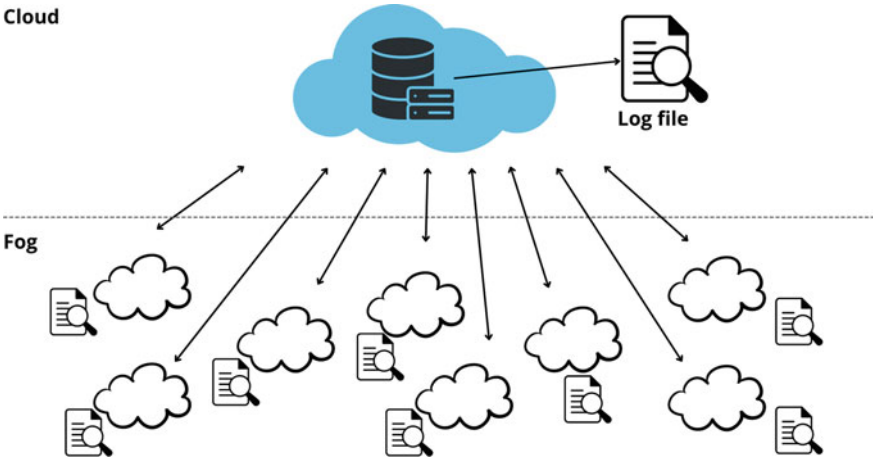

Fig. 4 Multiple fog nodes (devices) from which logs need to be collected, compared to one log file on cloud server. Based on [27]

3. data complexity and volume—currently, many fog devices collect as many data as possible (often send it further for cloud computing). In some cases, such a large amount of data is unstructured. It is a big challenge for the investigators to extract useful information from such big data portions. Usually, such process requires time-stamping and correlating obtained data with other information in order to make certain conclusions.
4. security mechanisms—forensic experts often need to decrypt data stored on fog layer devices, which may require additional computing resources.

Despite the technical aspects, fog layer devices may also collect sensitive data (e.g., medical and personal information), which are protected under different laws. Forensic experts in order to get access to such information need to obtain certain permissions, which may also slow down the data acquisition and investigation process.

3 Conclusions

There is a tremendous increase in the number of IoT devices in the last decade. IoT devices and sensors have become a requisite in most of the sectors including healthcare, transportation, agriculture, and so on. With the increase in such devices, there is also a huge explosion of data that is being generated every day. Computation of data over fog is revolutionary IoT. The enormous increase in data has led to increase in cyberattacks, hence the need of digital forensics for fog computing. Most of the digital forensics processes and principles that are being used by the law enforcement agencies are not suitable when fog computing and IoT is in picture. In this work, we have summarized the existing state-of-the-art forensic methods and principles that

can be applied and is compatible with fog computing and IoT devices. This work can potentially be used by researchers and technology experts around the world to develop new and advanced intelligent forensics methods that can be applied to IoT and fog computing.

Acknowledgements Research was sponsored by the Army Research Office and was accomplished under Grant Number W911NF-21-1-0264. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Office or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for government purposes notwithstanding any copyright notation herein.

References

1. Global IoT market forecast [in bilion connected IoT deviced] https://iot-analytics.com/number-connected-iot-devices/. Accessed 12 Oct 2022
2. Mell P, Grance T (2011) The NIST definition of cloud computing, p 7
3. 2021 IoT security landscape, https://securingsam.com/2021-iot-security-landscape/. Accessed 10 Oct 2022
4. How well do you know digital forensics? https://www.eccouncil.org/what-is-digital-forensics/. Accessed 12 Oct 2022
5. Fog computing market size, share and trends analysis report. https://www.grandviewresearch.com/industry-analysis/fog-computing-market/. Accessed 13 Oct 2022
6. Hegarty R, Taylor M (2021) Digital evidence in fog computing systems. Comput Law Secur Rev 41:105576
7. Hwaitat AKA, Manaseer SS, Al-Sayyed RMH (2019) A survey of digital forensic methods under advanced persistent threat in fog computing environment
8. 2022 sonicwall cyber threat report. https://www.sonicwall.com/2022-cyber-threat-report/. Accessed 12 Oct 2022
9. Hwaitat AKA, Manaseer SS, Al-Sayyed RMH (2020) An investigation of digital forensics for shamoon attack behaviour in fog computing and threat intelligence for incident response
10. Huang C, Lu R, Choo K-KR (2017) Vehicular fog computing: architecture, use case, and security and forensic challenges. IEEE Commun Mag 55(11):105–111
11. What's driving the connected car. https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/whats-driving-the-connected-car. Accessed 12 Oct 2022
12. A driverless future depends on data. https://blog.equinix.com/blog/2020/06/03/a-driverless-future-depends-on-data/. Accessed 12 Oct 2022
13. Big data on wheels. https://www.statista.com/chart/8018/connected-car-data-generation/. Accessed 12 Oct 2022
14. Brooks R, Iyengar S (1996) Robust distributed computing and sensing algorithm. Computer 29(6):53–60
15. Lai C, Lu R, Zheng D, Li H, (Sherman) Shen X (2016) Glarm: group-based lightweight authentication scheme for resource-constrained machine to machine communications. Comput Netw 99:66–81. https://www.sciencedirect.com/science/article/pii/S1389128616300238
16. Hu H, Lu R, Huang C, Zhang Z (2016) Tripsense: a trust-based vehicular platoon crowdsensing scheme with privacy preservation in vanets. Sensors 16(6). https://www.mdpi.com/1424-8220/16/6/803
17. Roopa M, Ayesha Siddiq S, Buyya R, Venugopal K, Iyengar S, Patnaik L (2021) DTCMS: dynamic traffic congestion management in social internet of vehicles (SIoV). Internet of Things 16:100311. https://www.sciencedirect.com/science/article/pii/S2542660520301426

18. Pattar S, Buyya R, Venugopal KR, Iyengar SS, Patnaik LM (2018) Searching for the IoT resources: fundamentals, requirements, comprehensive review, and future directions. IEEE Commun Surv Tutor 20(3):2101–2132
19. Mutlag AA, Abd Ghani MK, Arunkumar N, Mohammed MA, Mohd O (2019) Enabling technologies for fog computing in healthcare iot systems. Future Gener Comput Syst 90:62–78. https://www.sciencedirect.com/science/article/pii/S0167739X18314006
20. Parimbelli E, Wilk S, Cornet R, Sniatala P, Sniatala K, Glaser S, Fraterman I, Boekhout A, Ottaviano M, Peleg M (2021) A review of AI and data science support for cancer management. Artif Intell Med 117:102111. https://www.sciencedirect.com/science/article/pii/S0933365721001044
21. Ahmad M, Amin M, Hussain S, Kang B, Cheong T, Lee S (2016) Health fog: a novel framework for health and wellness applications. J Supercomput 72:10
22. Moosavi SR, Gia TN, Nigussie E, Rahmani AM, Virtanen S, Tenhunen H, Isoaho J (2016) End-to-end security scheme for mobility enabled healthcare internet of things. Future Gener Comput Syst 64:108–124. https://www.sciencedirect.com/science/article/pii/S0167739X16300334
23. Ao B, Wang Y, Yu L, Brooks RR, Iyengar SS (2016) On precision bound of distributed fault-tolerant sensor fusion algorithms. ACM Comput Surv 49(1):5:1–5:23. https://doi.org/10.1145/2898984
24. Iyengar SS, Ramani SK, Ao B (2019) Fusion of the Brooks-iyengar algorithm and blockchain in decentralization of the data-source. J Sensor Actuator Netw 8(1):17. 1 Publisher: Multidisciplinary Digital Publishing Institute. https://www.mdpi.com/2224-2708/8/1/17
25. Gundersen JH (2022) Digital forensics on fog-based IoT devices. Master's thesis in Information Security
26. Al-Masri E, Bai Y, Li J (2018) A fog-based digital forensics investigation framework for IoT systems. In: IEEE international conference on smart cloud (SmartCloud). IEEE, pp 196–201
27. Mukherjee M, Ferrag MA, Maglaras L, Derhab A, Aazam M (2019) Security and privacy issues and solutions for fog